PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-311220
(43)Date of publication of application : 07.11.2000

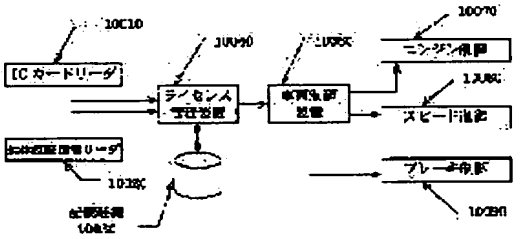
(51)Int.Cl. G06K 17/00
B42D 15/10
G06T 7/00
G06K 19/00
G06K 19/10
G07F 7/08

(21)Application number : 11-122395
(22)Date of filing : 28.04.1999

(71)Applicant : HITACHI LTD
(72)Inventor : SHIMIZU HIROSHI
KOMATA TAKASHI
MATSUMOTO KENJI

(54) UNIT OPERATION RIGHT MANAGING SYSTEM, UNIT OPERATION RIGHT MANAGING TERMINAL, IC CHIP AND IC CHIP CASE

(57)Abstract:
PROBLEM TO BE SOLVED: To certify the identify of a license operating a unit and a possessor of the license by recognizing the matching of a person having right, who is listed in a permission display means, and an operator operating the unit through the use of human body certification information on the operator.
SOLUTION: An IC card reader 10010 exists in a vehicle and a driver inserts a self-IC card into the IC card reader 10010 when he or she drives the vehicle. A human body certification information reader 10020 reads human body certification information showing ID of a human himself (herself) such as the fingerprint or the iris/retina of the driver seated on a driving seat. A license managing device 10040 compares processor information of a license which is read from the IC card with human body recognition information of the driver seated on the driving seat and judges whether they are same or not. When the driver seated on the driving seat is judged to be the person himself (herself) having qualification for driving the vehicle, the license managing device 10040 sends a message showing operation permission to a vehicle controller 10060.



LEGAL STATUS

[Date of request for examination] 22.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The right managerial system of device actuation characterized by to check coincidence with the rightful claimant indicated by said authorization display means and the operator who operates a device using an operator's biometrics information in the right managerial system of device actuation possessing an authorization display means to display the right which deals with a device, and an appliance control means to control the propriety of a device of operation.
[Claim 2] It is the right managerial system of device actuation characterized by carrying IC chip with which said authorization display means has memory or CPU in the right managerial system of device actuation according to claim 1.
[Claim 3] It is the right managerial system of device actuation characterized by said biometrics information being fingerprint information in claim 1 or the right managerial system of device actuation given in 2.
[Claim 4] The right managerial system of device actuation characterized by forming the sensor which detects said biometrics information on the switch which operates a device first in the right managerial system of device actuation according to claim 3.
[Claim 5] It is the right managerial system of device actuation characterized by being the information said biometrics information indicates a retina or an iris configuration to be in claim 1 or the right managerial system of device actuation given in 2.
[Claim 6] The right managerial system of device actuation characterized by installing the sensor which detects said biometrics information in the panel which displays the status information of a device in the right managerial system of device actuation according to claim 5.
[Claim 7] The right managerial system of device actuation characterized by installing the reader of said authorization display means, and the sensor which detects said biometrics information in an actuation device in claim 1 or the right managerial system of device actuation given in 2.
[Claim 8] The right managerial system of device actuation characterized by installing the reader of said authorization display means, and the sensor which detects said biometrics information in the personal digital assistant equipment of another object with an actuation device in claim 1 or the right managerial system of device actuation given in 2.
[Claim 9] The right managerial system of device actuation characterized by having the storage which memorizes said biometrics information in an actuation device in claim 1 or the right managerial system of device actuation given in 2.
[Claim 10] The right managerial system of device actuation characterized by memorizing said biometrics information for IC chip carried in said authorization display means in the right managerial system of device actuation according to claim 2.
[Claim 11] Said biometrics information memorized in the right managerial system of device actuation according to claim 10 is a right managerial system of device actuation which the number of is [two or more] and is characterized by the device to operate being freely selectable respectively in said biometrics information used for collating.
[Claim 12] The right managerial system of device actuation characterized by making it change to claim 1 or 2 in the right managerial system of device actuation of a publication according to the class of device which operates the authentication precision of said biometrics information.
[Claim 13] The right managerial system of device actuation characterized by attesting said biometrics information for before [every] starting of a device in claim 1 or the right managerial system of device actuation given in 2.
[Claim 14] The right managerial system of device actuation characterized by attesting said biometrics

information with a fixed time interval after starting of a device in claim 1 or the right managerial system of device actuation given in 2.
[Claim 15] The right managerial system of device actuation characterized by performing authentication of said biometrics information in claim 1 or the right managerial system of device actuation given in 2 for every time of the closing motion of a door which gets into [a device].
[Claim 16] The right managerial system of device actuation characterized by attesting said biometrics information for every time of termination of a device of operation in claim 1 or the right managerial system of device actuation given in 2.
[Claim 17] The right managerial system of device actuation characterized by to have the storage which memorizes at least one or more ID numbers indicated by said authorization display means published to those who have got actuation authorization of a device in the right managerial system of device actuation possessing an authorization display means display the right which deals with a device, and an appliance-control means control the propriety of a device of operation.
[Claim 18] It is the right managerial system of device actuation which said authorization display means is constituted by non-electronic means, such as paper, and said ID number is optically indicated on this authorization display means by the gestalt which can be read in the right managerial system of device actuation according to claim 17, and is characterized by for said appliance control means to have a reading means to read the ID number indicated by said authorization display means.
[Claim 19] The right managerial system of device actuation characterized by making actuation of a device impossible in claim 17 or the right managerial system of device actuation given in 18 unless the ID number indicated for said authorization display means is in agreement with the ID number memorized by the storage within said appliance control means.
[Claim 20] The right managerial system of device actuation characterized by giving an addition or the actuation authorization of a procedure changed or deleted for an ID number new to said storage at those who have said authorization display means of the ID number memorized by the storage within said appliance control means in the right managerial system of device actuation of any one publication of 19 from claim 17, and the congruous ID numbers.
[Claim 21] In the right managerial system of device actuation possessing an authorization display means to display the right which deals with a device, and an appliance control means to control the propriety of a device of operation It has a reading means to read the operational device information indicated by said authorization display means. Said appliance control means The right managerial system of device actuation characterized by judging whether said operational device information indicated by said authorization display means is in agreement with an own device, and enabling actuation of a device if in agreement.
[Claim 22] It is the right managerial system of device actuation which said authorization display means is constituted by non-electronic means, such as paper, and said operational device information is optically indicated on this authorization display means by the gestalt which can be read in the right managerial system of device actuation according to claim 21, and is characterized by for said appliance-control means to have an optical reading means read the operational device information indicated by said authorization display means.
[Claim 23] The right managerial system of device actuation characterized by changing the operational range of a device according to said operational device information in the right managerial system of device actuation according to claim 21.
[Claim 24] IC chip carried in said authorization display means in the right managerial system of device actuation according to claim 2 is a right managerial system of device actuation characterized by being the CPU card which can perform two or more applications.
[Claim 25] It is the right managerial system of device actuation characterized by being the card with which said CPU card includes a cybermoney function in the right managerial system of device actuation according to claim 24.
[Claim 26] IC chip carried in claim 2 or 24 in the right managerial system of device actuation of a publication at said authorization display means is a right managerial system of device actuation characterized by it being possible to record information, such as a location accompanying migration of a device and time of day which arrived at this location, when devices are boarding and a movable device.
[Claim 27] The right managerial system of device actuation characterized by performing a use limit of a device as the penalty for the violation of the Ruhr in use of a device etc. in claim 2 or the right managerial system of device actuation given in 24.
[Claim 28] It is the right managerial system of device actuation characterized by it being possible for said

penal regulations to carry out a multiple-times setup of the licence of a device and the setup of a disable along with a time-axis including prohibition of a fixed period of device actuation in the right managerial system of device actuation according to claim 27.
[Claim 29] Along with a time-axis, it is the right managerial system of device actuation characterized by it being possible to set up a use functional limit of a device over multiple times including the licence of a device, and prohibition including a limit of a function [in / on claim 27 or the right managerial system of device actuation given in 28, and / in said penal regulations / device actuation].
[Claim 30] The clock which manages said penal-regulations enforcement stage in the right managerial system of device actuation of any one publication of 29 from claim 27 is a right managerial system of device actuation characterized by making it impossible for the user of a device to change using information other than the guaranteed time information.
[Claim 31] IC chip which is an IC chip which has device actuation authorization information, and is characterized by indicating an owner's ID number and operational device information on an IC card that it has device actuation authorization for this IC chip.
[Claim 32] IC chip characterized by indicating biometrics information, such as a fingerprint of the owner of an IC card who has device actuation authorization for said IC chip, and a retina, the iris, in IC chip according to claim 31.
[Claim 33] IC chip characterized by including a cybermoney function in said IC chip collectively in IC chip according to claim 31.
[Claim 34] IC chip characterized by recording information, such as a location accompanying migration of a device, and time of day which arrived at this location, in IC chip according to claim 31 at said IC chip when devices are boarding and a movable device.
[Claim 35] IC chip characterized by including the information which can carry out a multiple-times setup of the licence of a device, and the setup of a disable in said IC chip along with a time-axis in IC chip according to claim 31 including the prohibition of a fixed period of the device actuation as penal regulations to the violation of the Ruhr in use of a device etc.
[Claim 36] IC chip characterized by including the information which can set up the use functional limits of a device including the licence of a device, and prohibition over multiple times as the penalty for the violation of the Ruhr in use of a device etc. along with a time-axis including a limit of a function in IC chip in IC chip according to claim 31.
[Claim 37] It is IC chip characterized by said IC chip being an IC chip in an IC card in IC chip of any one publication of 36 from claim 31.
[Claim 38] It is IC chip characterized by being built in the key with which said IC chip puts a device into operation in IC chip of any one publication of 36 from claim 31.
[Claim 39] It is IC chip which contains the clock which manages said penal-regulations enforcement stage for said IC chip in IC chip of any one publication of 36 from claim 31, and is characterized by making it impossible for the user of a device to change using information other than the time information this clock was guaranteed to be.
[Claim 40] The life of the cell which drives said clock in IC chip according to claim 39 is an IC chip which is in the term of device actuation authorization, abbreviation, etc. by carrying out, and is characterized by being a life.
[Claim 41] The right administration terminal of device actuation carry out having the storage which memorizes at least one or more ID numbers indicated by said authorization display means which published to those who have got actuation authorization of a device in the right administration terminal possessing a reading means read the information which indicated for an authorization display means display the right which deals with a device, and an appliance-control means control the propriety of a device of operation of device actuation as the description.
[Claim 42] The right administration terminal of device actuation characterized by giving an addition or the actuation authorization of a procedure changed or deleted for an ID number new to said storage at those who have said authorization display means of the ID number memorized by said storage in said right administration terminal of device actuation, and the congruous ID numbers in the right administration terminal of device actuation according to claim 41.
[Claim 43] It is IC chip case which is IC chip case having IC chip which consisted of semiconductor memory or a CPU, and is characterized by said IC chip in an IC card consisting of configurations which covered the whole external surface of said insulator with the conductor so that it may be sealed with the insulator except for a part for an electric contact surface and only the outcrop of the electric contact of said

IC chip may be removed.
[Claim 44] IC chip case characterized by said insulator surely existing in IC chip case according to claim 43 between the straight lines which connect said conductor to the outcrop of the electric contact of said IC chip.

[Claim 45] An authorization display means which builds in IC chip which consisted of semiconductor memory or a CPU to display the right which deals with a device, In the right managerial system of device actuation possessing this display authorization means and an appliance control means to have a connectable interface and to control the propriety of a device of operation said IC chip It has the function to perform informational encryption and decryption. To said interface The right managerial system of device actuation characterized by performing the communication link between IC chip which carried IC chip or application software which has a function equivalent to said IC chip, and was built in said authorization display means, and said interface with the enciphered signal.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] the device which has the function which writes the right of the license card type voice especially represented by the license of an automobile etc. of device actuation about the technique in connection with the right managerial system of device actuation with which this invention manages and controls the propriety of actuation of a device, and this device -- cooperating -- a device operator -- it is related with the technique in connection with the right managerial system of device actuation have the function which collates using biometrics information that he is him.
[0002]
[Description of the Prior Art] The certificate proving having the right which operates a device is published, and a right management method of device actuation to which only those who hold the certificate enable actuation of the device concerned is used by every place. For example, promptly, when it has the right to which only a person with a license drives an automobile in the case of a driver's license and presentation directions of the driver's license by the policeman come out, when not followed, it is real-applied according to this, using penal regulations as a **** system.
[0003] However, except when there are presentation directions of a policeman, even if an automobilism license does not demonstrate the effect and does not have a license, in fact, the automobilism is possible and has come to manage the right of device actuation certainly.
[0004] In order to solve this problem, with the technique indicated by JP,6-87285,A An IC card is used as a driver's license. To this IC card The matter indicated by licenses, such as ID of a driver, is filled in as electronic intelligence. The terminal which reads this information is prepared in an automobile, unless it is an effective license, this automobilism is made not to be made, and operation record is filled in in an IC card, and the method which totals the operation situation of each driver behind is indicated.
[0005]
[Problem(s) to be Solved by the Invention] It is that an automobile always distinguishes the license which did not have effect in the technique indicated by the above-mentioned prior official report except when showing a policeman, and the positive employment as a license in which the right which drives an automobile is shown is attained, taking advantage of the description of the memory function of an IC card, the log of an operation situation is taken collectively, and it becomes possible for you to also make it reflected in the optimal schedule.
[0006] However, with the technique indicated by said prior official report, there is a problem as shown below and consideration of these points is not made.
[0007] ** In said prior official report, any consideration is not probably paid about those who inserted the IC card license in the automobile checking truly whether you are the owner of a license, either. Therefore, operation will become possible, even when the person and operator who received handing out of a license are not the same people, namely, if those by whom license is not given in fact are also doing even possession for the license.
[0008] ** In said prior official report, about the correspondence when a license being invalidated by violation of traffic regulations etc. again Using data control equipment at the time of a traffic accident or a violation of traffic regulations, and writing in accident and violation data in a license at it, a summons document, and a fine statement of payment are published, The description about making it the engine not start during a license halt / lapse, although a license is inserted in the terminal of an automobile Or a certain thing, These are not made by using an IC card according to the present license employment approach about examination which applied the merit obtained for the first time to penal regulations.

[0009] ** In said prior official report, it has ID list of drivers who can drive this automobile to the IC card terminal of an automobile, and although the purport which only the driver who is in agreement with this ID can operate is indicated, about cooperation with the class of license, the class of automobile which can be driven, and an operation mode class, that examination is not made at all again.
[0010] ** In said prior official report, any consideration is not further paid about protecting to illegal modification of the contents of an IC card, either.
[0011] The place which this invention was made in view of the above-mentioned point, and is made into the purpose is to certainly enable authentication of being [which operates a device] a license, and the owner being the same. Moreover, about the actuation limit at the time of breaking actuation, the place made into the purpose of this invention is fine, and is to carry out as [be / the treatment which met parenchyma more / possible]. moreover -- being possible in the place made into the purpose of this invention setting up a limit of device actuation finely with the level of a license -- carrying out -- with -- **** -- it is in enabling it management of a trustworthy device operator and to prevent an operation mistake. Moreover, the place made into the purpose of this invention is using a CPU card, and is to prevent destruction of the card by software other than physical destruction.
[0012]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, in this invention, the following means are used, for example.
[0013] (1) the operation digiti manus which got on while preparing the terminal which inserts the license which has an IC card or an equivalent function in the automobile -- establish the detection means of the biometrics information which detects biometrics information, such as a crest and the iris, and indicate the information which expresses the biometrics information of the owner of a license with the memory of the license which has said IC card or equivalent function.
[0014] (2) Especially, in the case of an automobile, if processing like a publication is received in said prior official report in response to violation during passing, an automobilism will become impossible and it will become unmovable [a vehicle] in the location from which violation was started. Then, by setting up finely the automobilism authorization pattern at the time of violation along with a time-axis in an IC card, for example, issue of actual license halt disposal is set up two days after, and the terminal of an automobile also operates along with the directions.
[0015] (3) The level of a license prescribes the mode of operation of the vehicle to drive. For example, in exclusive courses and parking lots, such as a training place, the license which can perform only transit of less than 10 km/h of rates is set up, and the terminal of an automobile also operates according to the directions.
[0016] (4) Make possible easy read-out of data without the need for cipher processing, preventing destruction of the card by software other than physical destruction by using a CPU card. The date of issue of license halt disposal the above (2) and given in (3) degree and license level can specifically be read, without using a cipher-processing chip special to the exterior, and destruction and an alteration of the information are prevented.
[0017]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing.
[0018] Drawing 1 is the block diagram showing the configuration of the right managerial system of device actuation concerning the 1st operation gestalt of this invention, and this operation gestalt is an example of application to the right managerial system of device actuation in an automobile. This system contains equipment with the appliance control function which controls the propriety of actuation of a device (here automobile), and the IC card as an authorization display means with the information which shows the right (it shall be a driver's license here, for example, what permits operation only in limited area, such as a training within a station, shall be included) which deals with a device at least.
[0019] In an automobile, it is the IC card reader 10010. In case it is and a driver drives an automobile, it is the IC card reader 10010 about an own IC card. It inserts. Biometrics information reader 10020 The biometrics information which shows human being's ID own [, such as a fingerprint of the driver who sat on the driver's seat, or the iris, a retina, etc.,] is read. License management equipment 10040 Said IC card reader 10010 It is said biometrics information reader 10020 as well as the information of the owner of the applicable license read in the IC card. The read biometrics information of the driver who sat on the driver's seat is compared, and it judges whether it is the same.
[0020] Store 10030 For example, when limiting the driver who may operate this car, that driver ID is

memorized. The driver ID of the inserted IC card is this store 10030. It is the car control device 10060 later mentioned when not in agreement with the memorized driver ID. Engine starting is controlled.
[0021] license management equipment 10040 The information and the biometrics information reader 10020 from an IC card which were inserted from -- the time of judging it as him who has rating for surely the driver who sat on the driver's seat driving this automobile using information -- license management equipment 10040 -- car control device 10060 The message which shows authorization of operation is sent.
[0022] Car control device 10060 Engine control system 10070 which controls engines including the propriety of engine starting according to this allowed message Speed control device 10080 which controls the limiter of the travel speed of an automobile Authorization directions of operation are sent to the brake operating unit 10090 which sets up actuation of ABS (Antilock Brake System), and level, respectively. Although it does not exist under the system of a setup of the full speed which engine starting was attained by this and followed the rating level of a driver, and the further present license, ON/OFF control of ABS is performed in the form where the workmanship of a driver was balanced.
[0023] Drawing 2 is the explanatory view in the right managerial system of device actuation of this operation gestalt having shown one example of system arrangement near the cockpit of an automobile.
[0024] 20000 It is a ** cockpit. It is the IC card insertion opening 20020 to the driver's seat right. The driver who exists and drives this automobile is this insertion opening 20020 about the IC card which is an own license. It inserts. Next, the fingerprint reading section-cum-engine start button 20030 By pushing, the fingerprint of a driver is read and authentication with the biometrics information on the driver indicated to the previous IC card is performed. and a crest -- the person who pushed the reading section-cum-the engine start button 20030 can put an engine into operation only after he recognizes that he is him whom surely an IC card shows.
[0025] At this time, it is a store 20050. By having ID list of drivers who may drive this automobile, collating with ID of the inserted IC card is performed, and like explanation of drawing 1 , with a driver without operation authorization, as actuation including engine starting of an automobile cannot be performed, the security of ********** can be secured.
[0026] As the check technique of biometrics information, they are a retina and the iris sensor 20010 to a speedometer location. There is also the approach of establishing. In this case, since it is undetectable using this sensor unless a driver sits on a driver's seat, it is the fingerprint reading section-cum-the previous engine start button 20030, for example. It becomes impossible for him to whom the IC card (license) was delivered to push from a passenger seat, and for people without a license to sit on a driver's seat, and to operate. Since, as for a speedometer, the look of a driver is just surely going to go and, as for a driver's seat, the location of the head is fixed mostly here, they are a retina and the iris sensor 20010. It is suitable for installing.
[0027] Moreover, the device used as a license here is an IC card, and is an IC card corresponding to the multi-application used with cybermoney etc. Applications, such as cybermoney and an electronic credit, can be made by this to live together in the same IC card, and it is the tariff automatic payment system 20040 from an automobile. Correspondence to the system which does some shopping by access under [, such as automatic tariff payment of a highway, a drive-through, and a gas station,] the conditions which have surely taken the automobile can also be performed.
[0028] Furthermore, even if the license used here uses the license by the conventional printed matter, without using an IC card, a license can be inserted in a card slot and it can judge that it is the license of the driver who has obtained operation authorization of this automobile by reading an ID number etc. with an image scanner. further -- store 10030 the driver according to a license and biometrics information with the conventional license system even if it does not use an IC card by recording the biometrics information on a driver -- even if it is also possible to perform collating with him and it uses not an IC card but the conventional license system as it is, the function of this invention is realizable.
[0029] Drawing 3 is the explanatory view showing one example of the internal configuration (internal configuration of IC chip carried in the IC card) of the IC card used in the right managerial system of device actuation of this operation gestalt.
[0030] IC card 30000 Carried IC chip 30005 It has two or more DFs (Dedicated File) in the low order by making MF30010 (Master File) into the root, and DF1 (30020) is used for a license and DF2 (30060) is used for cybermoney. Under DF1 (30020), two or more EF(s) (Elementary File) are, and the information relevant to an electronic license is indicated. There are the fingerprint information, iris information, etc. that biometrics information is indicated to be a license ID number in EF1 (30030). In this case, biometrics information is the biometrics information reader 10020 with which may exist and the terminal of an automobile was equipped. For example, what is necessary is just to use iris information using fingerprint

information, if it is an iris sensor when it is a fingerprint scanner. [two or more kinds of] Violation hysteresis is indicated by the license class and level of this license, and EF3 (30050) at EF2 (30040). Only when DF and EF are a program and input a specific command from the outside, a CPU card can read biometrics information or can rewrite violation hysteresis. Only the software of dedication and the chip of dedication mentioned later can perform this specific command, it can maintain the secrecy of the internal information of a card by this, and can prevent an alteration.

[0031] Moreover, it is a clock 30070 in a card here. It prepares, and like said biometrics information and violation hysteresis, unless the software and the chip of dedication are mind, in case penal regulations issue at the time of the violation later mention in drawing 4 is enforce according to the date by consider as the mechanism in which the date and time of day of this clock are unchangeable, an action which puts a clock out of order intentionally and escapes penal regulations issue can be prevent completely. Although deviation naturally arises for the clock which operates alone on a card, this corrects the deviation of the clock in a card using the right time of day checked by the clock which the software or the chip of dedication can trust certainly [GPS etc.], when a card is inserted in a mounted terminal. When correction of this time of day may be made in the communication link at the time of the tariff automatic payment shown not only in the terminal carried in the automobile but in drawing 2 , and it cooperates with a cybermoney terminal regardless of an automobile and shopping by cybermoney or the electronic credit is performed, a clock may be corrected at any time from a terminal. Moreover, even if the drive power source of an IC card is not given from the outside to the clock installed in the IC card, it needs to operate, and it contains a thin cell in an IC card. although the life of this cell is fundamentally made into the life more than the authorization term of license -- a case -- the authorization term of license, and abbreviation -- you may make it have a comparable life Since none of this cell is used except the drive of a clock, it does not occur but the phenomenon in which a life becomes short according to a service condition can set up a life correctly.

[0032] Drawing 4 is front drawing showing one example of the penal-regulations processing pattern at the time of the violation in this operation gestalt.

[0033] the mode of operation at the time of driving an automobile with this operation gestalt as a pattern of penal-regulations processing -- (1) engine starting -- transit below (2) 10 km/h, and (3) -- it classified into three it can usually run. For example, in not breaking, though natural, it is possible to use all of these three modes of operation.

[0034] First, the speeding offense equivalent to the conventional license halt is shown. It will also be actually possible to continue riding as it is, if it will ride as it is when a speeding offense is carried out, for example in the middle of a travel, although the penal regulations, i.e., a license halt, according to a speeding offense with the conventional license were published instancy, and it will return and it is not further found by the police. When violation information is indicated as electronic intelligence by an IC card etc., the terminal corresponding to this is prepared in an automobile and a license halt is published instancy there, on that spot, during half a year, it becomes impossible to move an automobile and the phenomenon of making a vehicle into desertion in the middle of a path occurs. With this operation gestalt, after carrying out a speeding offense, issue of the penal regulations is set up from for example, two days after the time of violation, and an automobile is brought home between them, or it lends out and returns to origin. Penal regulations actual on it are published and processing whose operation is impossible can be carried out with this license.

[0035] Moreover, at least, when such an unusual speeding offense that a license halt is required instancy is performed, only a fixed period only of transit of 10 or less km/h for example, for two days is made possible, and prohibition of usual transit of an ordinary road is published from the roadside on the service area of a highway, instancy up to parking area, so that migration of a vehicle can be performed.

[0036] Moreover, since it is necessary to stop transit of a vehicle instancy at least at the exposure time in the license halt issue by alcoholic smell **** operation, of course, engine starting of an automobile of transit of 10 or less km/h is also made impossible. As a period until this comes [which was exposed] from drunkenness to its senses, it considers as prohibition of perfect operation only for 6 hours, and after that, after two days usually make transit possible and it brings a vehicle home like the above mentioned speeding offense, a license halt is published for the first time. According to the distance and the extenuation to the house of a driver, the person in charge who exposed can determine this period.

[0037] In addition, the limitation according to the penal regulations written in an IC card can set up licence, a disable, a use functional limit, etc. over multiple times along with a time-axis.

[0038] Although the stage and time of day of the penal-regulations issue in this operation gestalt are enforced according to the clock used as a certain criteria, if a driver changes the clock freely, for example, a

clock is set forward half a year, when the clock carried, for example in the usual automobile is used, since the disposal period has already passed, it will become possible to operate freely. In order to prevent this, as shown in drawing 3 , it may have the clock which cannot change time of day freely from the outside in an IC card, or the clock which cannot perform a time-of-day setup of arbitration at all may be given to a mounted terminal except correcting time of day by the clock reliable certainly [the same function, i.e. GPS etc.,].

[0039] Drawing 5 is front drawing in the right managerial system of device actuation concerning the 2nd operation gestalt of this invention which described one example of a convention of the mode of operation by the license class. This operation gestalt is an example supposing operation of a HEL, and indicates the mode of operation to each to be a license of the pilot wave of a normal license, a trainee, and each mechanic.

[0040] The pilot wave of a normal license can perform engine starting, hovering, slow flights, and all the high-speed flights, though natural. In the case of a trainee, from engine starting to a slow flight can carry out, and it has the limit to a high-speed flight. concrete -- for example, a main rotor -- the control which cannot lean the include angle of surface of revolution more than fixed of a pilot wave's volition is put in. of course, the automatic attitude control with a gyroscope etc. can be pushed down until include-angle full, without receiving this limit Moreover, the 1st class of the mechanic with rating which can perform an easy surfacing trial presupposes that it is possible to engine starting and hovering. concrete -- extent in which even front and rear, right and left migration of super-low ** is possible -- for example, a main rotor -- control it becomes impossible to modification operate [of the include angle of surface of revolution] is performed. In the case of the 2nd class of a mechanic only with maintenance rating, it is only engine starting.

[0041] Although the concrete limit technique of such control changes with devices to control, in case an automobile is driven by setting up how far it can be operated with the license, control which changes a mode of operation within an ordinary road and an exclusive course is possible also for the same temporary license at the device side which indicates the level of a license to IC card license, and is actually operated to it.

[0042] Drawing 6 is the 1st example of the flow chart which showed the operating procedure at the time of operating a device in the right managerial system of device actuation by this invention.

[0043] First, an ID card is inserted in the device to operate (step 60010), and then a fingerprint is inputted (step 60020). Next, step 60030 The coincidence of fingerprint information inputted as the fingerprint information indicated by the inserted ID card is judged, and those who inputted the fingerprint judge that he is the owner of an ID card. It is Eject of an ID card, performing a display of that it cannot operate, if a judgment is x. It carries out (step 60040). If the device which will perform an engine start (step 60050) and will be controlled if a collating result is O is an automobile, it will run (step 60060).

[0044] As described above, an ID card here not only in what is constituted with IC chip with memory The fingerprint information corresponding to an applicable license number is read from the storage carried in the device which read the license number of the license of the printed matter by which present condition use is carried out etc. with the image scanner, and was shown by drawing 1 and drawing 2 . A coincidence judgment with the fingerprint which the pilot inputted may be made, and the function that the present printed matter license is also equivalent can be attained in this case.

[0045] Drawing 7 is the 2nd example of the flow chart which showed the operating procedure at the time of operating a device, and the 3rd example in the right managerial system of device actuation by this invention.

[0046] (a) of drawing 7 is a flow chart in the case of collating the class of an ID card and device to control. First, a pilot inserts an ID card in a device (step 70010), and the device to control reads License ID in the inserted ID card. And it judges that it is the license whose applicable license ID can control this device (step 70020), when operation is impossible, an operation improper display is performed, and it is Eject of an ID card. It carries out (step 70030). If the device which will perform an engine start (step 70040) and will be controlled if a collating result is O is an automobile, it will run (step 70050).

[0047] As the ID card was described above here, the license number of the license of what [not only] is constituted with IC chip with memory but the printed matter by which present condition use is carried out, and the class of device which can be controlled indicated can be read with an image scanner, you may judge that it is the license which can control this device, and the function that the present printed matter license is also equivalent can be attained in this case.

[0048] (b) of drawing 7 is a flow chart which shows the example which realized the function of both drawing 6 and drawing 7 of (a). That is, a pilot inserts an ID card in a device (step 70010), and then inputs a fingerprint (step 70060). Next, step 70070 The coincidence of fingerprint information inputted as the

fingerprint information indicated by the inserted ID card is judged, and those who inputted the fingerprint judge that he is the owner of an ID card. It is Eject of an ID card, performing a display of that it cannot operate, if a judgment is x. It carries out (step 70031). It judges that it is the license with which the license ID read in the inserted ID card when the collating result was O can control this device (step 70021), when operation is impossible, an operation improper display is performed, and it is Eject of an ID card. It carries out (step 70032). If the device which will perform an engine start (step 70041) and will be controlled if a collating result is O is an automobile, it will run (step 70051).

[0049] The mechanism in which the police etc. is told about existence of an offender here using the means of communications which the driver the automobile has got into [driver] at this collating time when the automobile has always received [in / for example / an automobile] a criminal's on the wanted list etc. license ID in the network etc. does not illustrate at the same time he recognizes that he is an offender etc. and performs an operation improper display although whichever is sufficient as the collating sequence of fingerprint authentication and License ID is also realizable. It becomes possible to detect a trustworthy offender by performing this procedure at the very first.

[0050] In addition, it may be made to perform authentication (collating) of biometrics information, such as fingerprint authentication, to the switching operation and coincidence of a door at the time of getting into [a vehicle] by preparing a sensor for identifying fingerprints in the handle of the predetermined door of vehicles, such as an automobile, etc. again.

[0051] Further again, it may be made to carry out after starting initiation authorization of a device for every fixed time amount, or it not only performs authentication (collating) of biometrics information, such as a fingerprint and the iris, for before [every] starting of devices, such as an automobile, but may be made to carry out for every time of termination of a device of operation. By doing in this way, after starting actuation of a device, a different person from the person who attested first can supervise whether operation, operation, etc. of a device were changed on the way. and when operation, operation, etc. are changed on the way, although it depends on the circumstances, stop actuation of a device gradually after warning, or [that devices, such as an automobile warn of this purport] Or it can also consider as structure which combines, and records or carries out automatic information of the information on having carried out the unjust shift of the information on having carried out the unjust shift, and the biometrics information of the person after a shift, and the biometrics information of the person after a shift outside at the storage of an IC card or a device. Therefore, in a taxi etc., when the malicious PAX captures a vehicle and operates, the effect is greatly demonstrated.

[0052] Drawing 8 is the explanatory view having shown the example of the operation gestalt of the remote control for starting the device which comes to equip applicable IC card reader and an applicable biometrics information reader in the right managerial system of device actuation by this invention.

[0053] The remote control shown in (a) of drawing 8 gives a function equivalent to mounted equipment (terminal unit) with the appliance control function in the above mentioned 1st operation gestalt by making remote control possess the fingerprint scanner as IC card reader and a biometrics information reader.

[0054] In the body of remote control, it is the starter [a fingerprint scanner-cum-] carbon button 80020. It is and a user is IC card 80030. It inserts. Carbon button 80020 A fingerprint is scanned by putting a finger and it is IC card 80030. Collating with the fingerprint information indicated inside and a user's scanned fingerprint information is performed. When collating is materialized, they are infrared radiation / electric-wave discharge opening 80010 for the first time. Signals, such as an engine start of an automobile and door-lock discharge, are discharged by infrared radiation or the electric wave.

[0055] (b) of drawing 8 is the example which built the function of an IC card in the interior of remote control. In the case of this example, it becomes a different use gestalt from the license of a general-purpose automobile, but since the fingerprint information of those with rating for moving that device is memorized when it is going to move a certain device, even if other persons are going to move a device, it cannot start. Moreover, since there is no plug of an IC card, loss by carrying of a card is also avoidable.

[0056] Drawing 9 is the explanatory view having shown the example of an approach which takes out licence to those who are not taking out the licence of a device in the right managerial system of device actuation by this invention. As a concrete example, the owner of a certain automobile explains the actuation flow for granting other men the right which drives the automobile based on an actuation screen.

[0057] First, as the actuation screen of (a) of drawing 9 shows, an automobile is urged to insertion of an ID card at owner, in order that surely those who give the operation authorization to others may judge that he is the owner of the vehicle. collating of biometrics information, such as a fingerprint which is not illustrated here, -- owner -- it checks that he is him.

[0058] Next, the operation authorization mode given to others is chosen on the actuation screen shown in (b) of drawing 9 . That is, an assignment date is specified by choosing "2" by choosing "1" only on the day. And a family's etc. permanent license is given by choosing "3." After this selection, on the same actuation screen as (a) of drawing 9 , insertion of the ID card of the driver who gives operation authorization is urged, and operation authorization is registered.
[0059] The screen of (c) of drawing 9 shows what displayed the list of the driver which has already been registered into this vehicle now, and which can be operated. By choosing by the number here, as shown in the actuation screen of (d) of drawing 9 , operation authorization mode can be changed.
[0060] Drawing 10 is the explanatory view having shown the example of the pattern changed by the device which controls the precision of authentication of biometrics information in the right managerial system of device actuation by this invention. As for authentication (collating) of biometrics information, by the method of fingerprint authentication, the following three methods are one of the present condition and typical things.
** . MANISHAA method which collates the location and direction of the branch point of the ridgeline of a fingerprint, and an endpoint.
** . MANISHAA relation method using relative physical relationship in addition to **. Although the amount of data and a processing load are large, it is used for the National Police Agency deducing a criminal.
** . Image chip method collated using the piece of an image containing the focus (chip).
[0061] The authentication precision as a method serves as order of **->**->**. Moreover, collating precision changes by which is sampled to the each, and if the number of samplings is raised, the processing time will start. Collating precision takes, and as a direction, about 15 focus is chosen and sequential collating of this is carried out, and if seven places are continuously in agreement, it will consider as collating ******, for example. Thus, when it is decided by where collating is stopped that collating precision will be the number of the focus, for example, all are collated, time amount may also be taken, on the contrary the rate of he collating may fall.
[0062] Although it is a target that the device which can be controlled according to the class of license is limited certainly fundamentally and it is an ideal, if authentication precision is raised according to the above-mentioned problem, the phenomenon in which the processing time does not start or it does not attest by him conversely, either will occur. the class of device to control -- him -- there are some which may lower the level of authentication and it becomes possible to correspond to improvement in processing speed, or reduction of cost.
[0063] The table of drawing 10 shows the type of a car to control, its significance, and the rating level of a license. C of significance is the lowest and it is [A] the highest. [of significance] Moreover, rating level has lowest E and those to whom A has the license of the highest and high level also have operation rating of a license of low level in coincidence. For example, if a license is usually set to D and the license of a bicycle with a prime mover is set to E, operation of a bicycle with a prime mover is also possible for the person with the license of D.
[0064] In the table of drawing 10 , significance is the device which almost all persons can control, if the bicycles with a prime mover of C are those to whom it has a license since the operation rating level is also the minimum E. Then, it is not necessary to also give authentication of biometrics information to a precision, and it has made biometrics level the minimum level "1."
[0065] The cost of a car of an automobile, or a taxi and a large-size car is also expensive, and since the effect by the theft is also large, they usually set significance to B. Since a standard-sized car is a general individual car in it, the rating level is D and a taxi is an operating car, the rating level is set to C. Since the magnitude of a car and the difficulty of operation of these two are the same, biometrics level is set as level "2" higher than a bicycle with a prime mover as the same.
[0066] Since it is large compared with said two cars and difficulty of operation is high, I hear that more positive rating is necessary (rating level B), and a large-size car sets biometrics level as still higher level "3."

[0067] And finally, I hear that an urgent automobile has the significance as highest as A, and only a specific rating person drives it, and it also sets rating level to the highest A. And biometrics level is set to the "4" in order to check a more positive driver, since the effect of [when a theft occurs] is the largest. [highest] In this case, since emergency service is needed, it is necessary to attest an urgent car certainly for a short time, without mistaking a qualified person to positive authentication and coincidence. For this reason, that to which the algorithm of biometrics was also suitable for it will be used.

[0068] Drawing 11 is the explanatory view having shown the example which records the passing root using the memory function of an IC card in the right managerial system of device actuation by this invention. That is, it is the explanatory view in which those who drive an automobile using the device actuation managerial system of said 1st operation gestalt shown in drawing 1 showed how to save the transit path as own record at an IC card.
[0069] (a) of drawing 11 shows the path which a driver follows. starting point 11040 from -- road 11030 passing -- crossing 11020 Y character branching 11010 after turning left turning left -- destination 11000 It arrives. This passing path is a crossing 11020 at the time of passing, although beforehand set up with the car-navigation system. A situation is photoed with an electronic camera (11060 shows this photography image). Arrow head 11070 piled up on the image It is the direction at which the automobile actually turned.
[0070] (b) of drawing 11 is the example of the format which records the passing path of a driver on the IC card of a driver. A crossing is mainly separated according to some checkpoints for a passing way, a starting point coordinate and a terminal point coordinate are written by lat/long, and the date and time of day which passed the starting point, and the time amount taken to pass through this root are indicated. Furthermore, the file name of the image photoed by (a) of drawing 11 is attached so that it may become an intersectional mark. This record is recorded on the storage of once mount during transit, and you may make it download it to an IC card finally.
[0071] it is possible to put the exact transit record which is not changed under management of the individual who ran with the privacy of an IC card (especially CPU card) by performing such record -- becoming -- individual management -- and -- for example, when the automobile of the same type of a car and an appearance causes a crime, self is not related to a crime by this record -- it also becomes possible to prove things.
[0072] Drawing 12 is the explanatory view showing the example of the operation gestalt which built the applicable function of an IC card in the key of an automobile in the right managerial system of device actuation by this invention.
[0073] (a) of drawing 12 is the example constituted so that the terminal of the automobile which is made to contain the IC chip 120020 in a key 120010, and inserts this key 120010 and key with the interface terminal 120030 might be connected. In this case, with a license, although gestalten differ, by putting in the ID number and biometrics information on a driver, as mentioned above in the lock itself, they are only use of the same key as the present condition, and can give the same effectiveness as use of an IC card.
[0074] (b) of drawing 12 is the example which made the fingerprint sensor 120040 build in a key 120011 further in addition to the function of the key 120010 of (a) of drawing 12 . In addition, in (b) of drawing 12 , 120021 is IC chip and 120031 is an interface terminal.
[0075] In the case of the example of (b) of this drawing 12 , a key 120011 can be inserted in the keyhole of an automobile and the same effectiveness as the above mentioned operation gestalt can be acquired by the completely same actuation as the present actuation of twisting and starting the engine. Here, the sensor which detects as information the distribution of load of the finger which changes delicately with individuals as a biometrics information sensor for which the fingerprint sensor 120040 is substituted may be used. Moreover, the gravity dependent opacity by the time-axis at the time of distribution of load also twisting not only the direction of a field but a key may be used as biometrics information. - with a key -- even if it does not use an advanced sensor called a fingerprint sensor by using actuation of twisting, it is possible to attest biometrics information.
[0076] Drawing 13 is the explanatory view having shown the pattern which limits the type of a car operated according to the class of license in the right managerial system of device actuation by this invention. Since a format of the table of drawing 13 is the same as that of drawing 4 and drawing 5 , explanation here is omitted.
[0077] The class of license shows trainee, temporary license, and book license and AT (automatic car) limitation. For example, the trainee who performs operation training within a station considers all as ** also including engine starting. This shows that operation is possible on the conditions what has this license in a passenger seat has got into [conditions], although actuation is possible. The certification of what has this license being in a passenger seat is a vehicle only for trainings, and after attesting by inserting this license in the terminal of a driver's seat in advance the same with the approach of installing the same IC card reader as a driver's seat in a passenger seat, and giving the operation authorization shown by drawing 9 R> 9, it has a method of giving a trainee operation authorization. The same is said of the operation authorization by temporary license.
[0078] Although operation of all automobiles can naturally perform this license, although transit of an

automatic-transmission car is possible, the transit of MT vehicle of the person of AT limited license becomes impossible according to the class of the license here. If a gear is put in, specifically, it will consider as a mechanism which carries out an engine stall so that a throttle may not open. However, transit by the Starter motor may be enabled for emergency egresses, or control which enables only transit of less than 10 km/h of rates for less than 5 minutes may be performed.

[0079] Drawing 14 is the explanatory view having shown the example of the operation gestalt of an IC card for setting to the right managerial system of device actuation by this invention, and preventing the electrostatic discharge of IC chip at the time of the IC card insertion to an applicable terminal unit.

[0080] 140060 is IC card insertion opening by the side of a terminal (terminal unit), and connects with the electrode by the side of an IC card by the connector 140061 at the time of insertion. The heart consists of insulators, the IC chip 140010 is enclosed, and, as for IC card 140000, only the polar zone is exposed to the front face. And space where a spark flies between a conductor and IC chip does not exist, but the configuration of an insulator 140020 is set up so that it may enter in the form which an insulator surely interrupts, so that, as for IC card 140000, the conductor 140030 may have covered the perimeter, a spark etc. may not arise between a conductor and IC chip and fixed spacing may open.

[0081] When a user has IC card 140000, a conductor 140030 is grounded through the body (140040). When inserting an IC card in a terminal, since between the road surfaces equivalent to a ground is insulated with the rubber tire, especially in the case of an automobile etc., a spark arises between the electrified automobile and the inserted IC card (140070). Potential of a terminal and an IC card is made equal by making it ground via the body through a conductor 140030 so that this spark may not flow into the IC chip 140010. Moreover, the electric conduction brush 140050 is formed in IC card slot within a terminal, and electric discharge on the front face of a terminal of an IC card, cleaning of dust, etc. are performed especially. Breakage of the IC card (IC chip) by high-voltage static electricity peculiar to an automobile can be prevented thereby especially.

[0082] Drawing 15 is the explanatory view having shown the example of the operation gestalt which performs confidentiality of the applicable information between a terminal (terminal unit) and an IC card in the right managerial system of device actuation by this invention.

[0083] The information between a terminal 150000 (terminal unit) and IC card 150100 is acting as a monitor, and can monitor the contact shown in drawing 14 . In analyzing the signal furthermore monitored, a false signal can be inputted from this contact and the IC card items mentioned can also be changed.

[0084] So, in this example shown in drawing 15 , a chip with a built-in CPU is used for IC chip of IC card 150100, and the signal which enciphered transfer of the signal between terminals 150000 performs. There is the chip 150010 with a built-in CPU which has a function equivalent to the chip built in the IC card in a terminal 150000 side, or exclusive application 150020, and the communication link with an IC card is performed via these chips or application. IC chip of built-in in IC card 150100, IC chip by the side of a terminal 150000, or application has encryption / decryption function by the same method, and prevents the alteration and forgery based on these certainly in wire tapping of commands, such as read-out of the information on IC card 150100, and rewriting, and information, and a list. A license number, a name, etc. are equivalent to the items mentioned of the usual license, and the information without the need of making it secret can read them through the through path 150030. In this case, information can be expressed as the terminal of very easy structure, for example like the balance display machine of cybermoney. Moreover, even if it does not perform cipher processing, use of a CPU chip enables it to use a specific command for write-in access to an IC card, and it becomes possible to prevent an operation mistake and destruction simple.

[0085] As mentioned above, although the mainly illustrated operation gestalt explained this invention, to say nothing of deformation various in the range which does not deviate from the pneuma of this invention to this contractor being possible, it is possible to use the thing of the type an IC card is made to possess the function in which the wireless transmission and reception between point-blank range are possible, and deliver and receive information by non-contact besides what deliver and receive information by the contact process as an IC card. In this case, it is possible to also make the function of IC chip of this invention build in pocket devices, such as a cellular phone and a wrist watch.

[0086]

[Effect of the Invention] According to this invention, a trustworthy device operator is manageable as mentioned above by attesting being [which operates a device] a license, and that the owner is the same. Moreover, the actuation limit at the time of breaking actuation can also perform fine processing in alignment with a time-axis, and can take the measures which met parenchyma more. Moreover, a limit of device

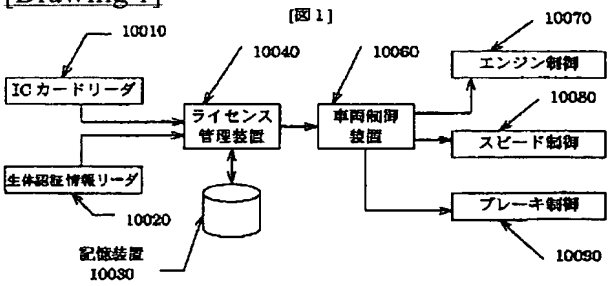
actuation can be set up finely and the level of a license enables it to prevent management of a trustworthy device operator and an operation mistake. Furthermore, it becomes possible about easy read-out of data without the need for cipher processing, preventing destruction of the card by software other than physical destruction by using a CPU card.

[Translation done.]

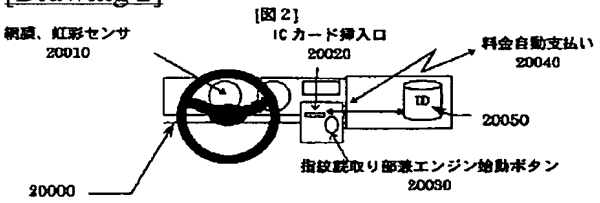
* NOTICES *

DRAWINGS

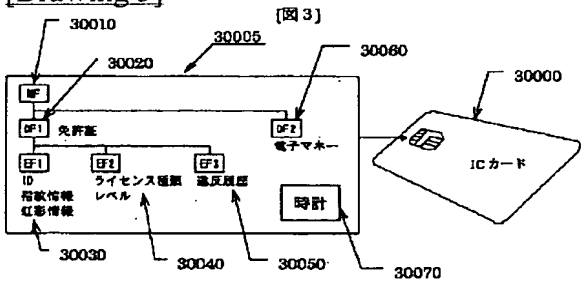
[Drawing 1]



[Drawing 2]



[Drawing 3]



[Drawing 4]

[図4]

#	事項	動作モード		
		エンジン始動	10km/h 未満	通常走行
1	無違反	○	○	○
2	スピード違反	○	○	○(但２日間)
3	重大スピード違反	○	○(但２日間)	×
4	酒気帯び運転	×(但６時間)	×(但６時間)	○ (但６時間以降２日間)

[Drawing 5]

[図5]

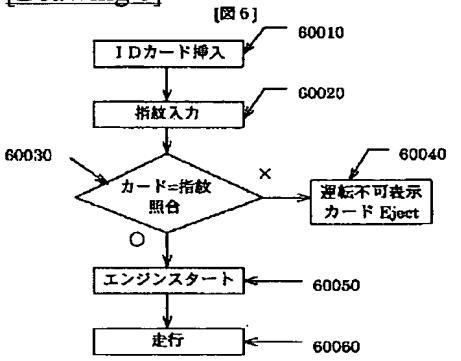
#	事項	動作モード			
		エンジン始動	ホバリング	低速飛行	高速飛行
1	パイロット	○	○	○	○
2	訓練生	○	○	○	×
3	メカニック１級	○	○	×	×
4	メカニック２級	○	×	×	×

[Drawing 10]

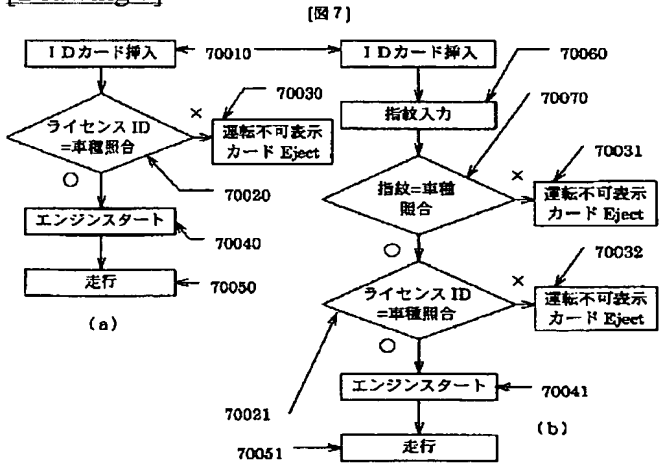
[図１０]

#	車種	ライセンス管理レベル		
		重要度	資格レベル	生体認証レベル
1	原動機付自転車	C	E	1
2	普通車	B	D	2
3	タクシー等	B	C	2
4	大型車	B	B	3
5	緊急自動車	A	A	4

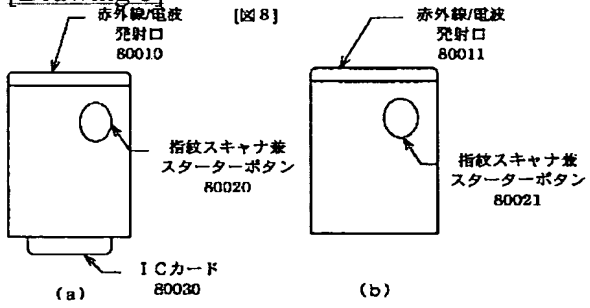
[Drawing 6]



[Drawing 7]

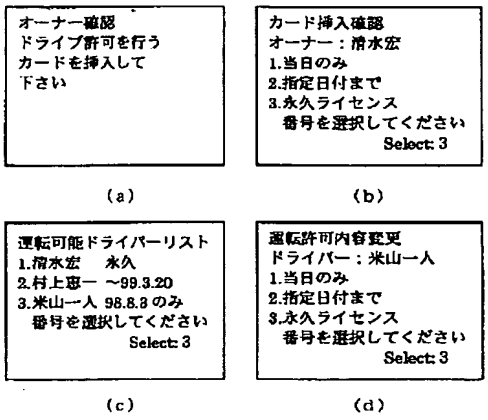


[Drawing 8]



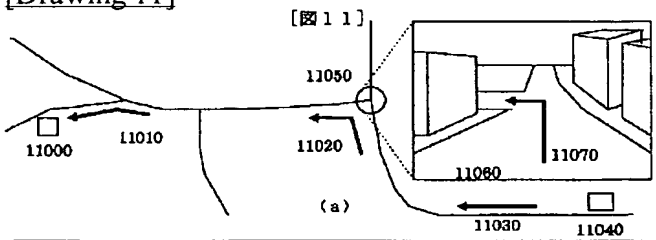
[Drawing 9]

[図9]



[Drawing 11]

[図11]

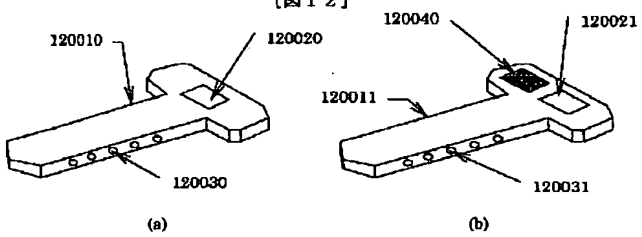


ルート#	終点座標	始点座標	日付	時刻	所要時間	画像ファイル名
1	110.25-540.12	111.32-538.00	H10.7.30	14:00	8分	W0001.GIF
2	111.32-538.00	112.21-535.86	H10.7.30	14:08	7分	W0002.GIF
.....						
8	120.00-532.65	122.37-533.77	H10.8.2	07:59	12分	W0008.GIF
.....						
22	131.88-525.07	130.02-522.98	H10.8.6	16:45	15分	W0022.GIF
23	130.02-522.98	129.25-521.45	H10.8.6	17:00	16分	W0023.GIF

(b)

[Drawing 12]

[図12]



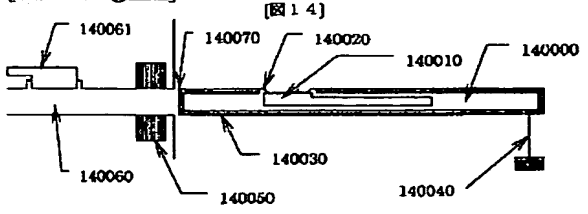
[Drawing 13]

[図13]

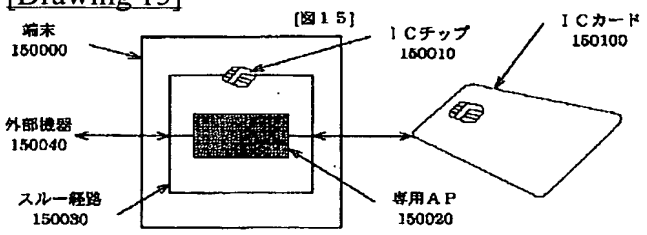
#	事項	動作モード		
		エンジン始動	MT	AT
1	練習生	△	△	△
2	仮免許	○	△	△
3	本免許	○	○	○
4	AT限定	○	×	○

[Drawing 14]

[図14]



[Drawing 15]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－311220
（P2000－311220A）
(43)公開日　平成12年11月７日(2000.11.7)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ	２Ｃ００５
Ｂ４２Ｄ　15/10	５２１	Ｂ４２Ｄ　15/10	５２１	３Ｅ０４４
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６５Ｋ	５Ｂ０３５
Ｇ０６Ｋ　19/00		Ｇ０６Ｋ　19/00	Ｔ	５Ｂ０４３
19/10			Ｓ	５Ｂ０５８

審査請求　未請求　請求項の数45　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－122395

(22)出願日　平成11年４月28日(1999.4.28)

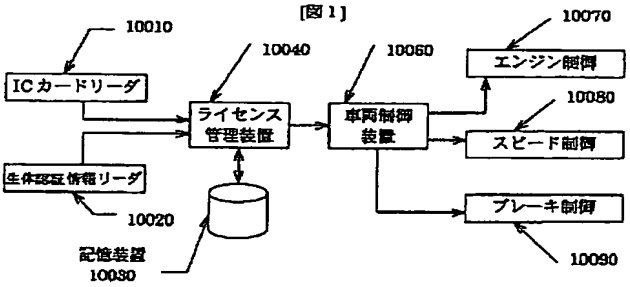
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　清水　宏
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　小俣　隆
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100078134
弁理士　武　顕次郎

最終頁に続く

(54)【発明の名称】　機器操作権管理システムおよび機器操作権管理端末およびＩＣチップおよびＩＣチップケース

(57)【要約】
【課題】　機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うようにすること。
【解決手段】　免許証としてメモリチップ等を搭載したＩＣカードなどを用い、自動車に、ＩＣカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋・虹彩等の生体認証情報を検知する生体認証情報検出手段を設け、また、ＩＣカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。そして例えば、運転者の生体認証情報と免許証記載の生体認証情報との照合が一致し、かつ免許証の内容が運転する自動車に合わない限り、運転を不可能とする。

[図１]



【特許請求の範囲】

【請求項１】　機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
前記許可表示手段に記載されている権利者と、機器を操作する操作者との一致を、操作者の生体認証情報を用いて確認することを特徴とする機器操作権管理システム。

【請求項２】　請求項１に記載の機器操作権管理システムにおいて、
前記許可表示手段は、メモリもしくはＣＰＵを有するＩＣチップを搭載していることを特徴とする機器操作権管理システム。

【請求項３】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報は、指紋情報であることを特徴とする機器操作権管理システム。

【請求項４】　請求項３に記載の機器操作権管理システムにおいて、
前記生体認証情報を検出するセンサを、機器を最初に作動させるスイッチ上に設けたことを特徴とする機器操作権管理システム。

【請求項５】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報は、網膜もしくは虹彩形状を示す情報であることを特徴とする機器操作権管理システム。

【請求項６】　請求項５に記載の機器操作権管理システムにおいて、
前記生体認証情報を検出するセンサを、機器のステータス情報を表示するパネルに設置することを特徴とする機器操作権管理システム。

【請求項７】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器内に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。

【請求項８】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器とは別体の携帯端末装置に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。

【請求項９】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
操作機器内に、前記生体認証情報を記憶する記憶装置を有することを特徴とする機器操作権管理システム。

【請求項１０】　請求項２に記載の機器操作権管理システムにおいて、
前記許可表示手段に搭載したＩＣチップに、前記生体認証情報を記憶することを特徴とする機器操作権管理システム。

【請求項１１】　請求項１０に記載の機器操作権管理システムにおいて、
記憶している前記生体認証情報は複数種であり、操作する機器が、照合に使用する前記生体認証情報をそれぞれ自由に選択可能であることを特徴とする機器操作権管理システム。

【請求項１２】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証精度を、操作する機器の種類に応じて変化させることを特徴とする機器操作権管理システム。

【請求項１３】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の起動前毎に行うことを特徴とする機器操作権管理システム。

【請求項１４】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の起動後に一定時間間隔で行うことを特徴とする機器操作権管理システム。

【請求項１５】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器に搭乗する扉の開閉時毎に行うことを特徴とする機器操作権管理システム。

【請求項１６】　請求項１もしくは２に記載の機器操作権管理システムにおいて、
前記生体認証情報の認証を、機器の動作終了時毎に行うことを特徴とする機器操作権管理システム。

【請求項１７】　機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
機器の操作許可を得ている者に発行した前記許可表示手段に記載されているＩＤ番号を、少なくとも１つ以上記憶する記憶装置を有することを特徴とする機器操作権管理システム。

【請求項１８】　請求項１７に記載の機器操作権管理システムにおいて、
前記許可表示手段は紙等の非電子手段により構成され、前記ＩＤ番号は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載されたＩＤ番号を読み取る読み取り手段を有することを特徴とする機器操作権管理システム。

【請求項１９】　請求項１７もしくは１８に記載の機器操作権管理システムにおいて、
前記許可表示手段に記載されたＩＤ番号が、前記機器制御手段内の記憶装置に記憶されているＩＤ番号と一致しない限り、機器の操作を不可能とすることを特徴とする機器操作権管理システム。

【請求項２０】　請求項１７から１９の何れか１つに記載の機器操作権管理システムにおいて、

前記機器制御手段内の記憶装置に記憶されているＩＤ番号と一致したＩＤ番号の前記許可表示手段を有する者に、前記記憶装置に新たなＩＤ番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理システム。

【請求項２１】　機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、

前記許可表示手段に記載されている操作可能機器情報を読み取る読み取り手段を有し、前記機器制御手段は、前記許可表示手段に記載されている前記操作可能機器情報が自身の機器と一致しているかの判断を行い、一致していれば機器の操作を可能とすることを特徴とする機器操作権管理システム。

【請求項２２】　請求項２１に記載の機器操作権管理システムにおいて、

前記許可表示手段は紙等の非電子手段により構成され、前記操作可能機器情報は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載された操作可能機器情報を読み取る光学的読み取り手段を有することを特徴とする機器操作権管理システム。

【請求項２３】　請求項２１に記載の機器操作権管理システムにおいて、

前記操作可能機器情報に従って、機器の操作可能範囲を変更することを特徴とする機器操作権管理システム。

【請求項２４】　請求項２に記載の機器操作権管理システムにおいて、

前記許可表示手段に搭載したＩＣチップは、複数のアプリケーションの実行が可能なＣＰＵカードであることを特徴とする機器操作権管理システム。

【請求項２５】　請求項２４に記載の機器操作権管理システムにおいて、

前記ＣＰＵカードは、電子マネー機能を含むカードであることを特徴とする機器操作権管理システム。

【請求項２６】　請求項２もしくは２４に記載の機器操作権管理システムにおいて、

前記許可表示手段に搭載したＩＣチップは、機器が搭乗および移動可能な機器である場合に、機器の移動に伴う位置や、該位置に到達した時刻等の情報を記録することが可能であることを特徴とする機器操作権管理システム。

【請求項２７】　請求項２もしくは２４に記載の機器操作権管理システムにおいて、

機器の使用におけるルール違反等に対する罰則として、機器の使用制限を行うことを特徴とする機器操作権管理システム。

【請求項２８】　請求項２７に記載の機器操作権管理システムにおいて、

前記罰則は機器操作の一定期間の禁止を含み、時間軸に沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能であることを特徴とする機器操作権管理システム。

【請求項２９】　請求項２７もしくは２８に記載の機器操作権管理システムにおいて、

前記罰則は機器操作における機能の制限を含み、時間軸に沿って、機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能であることを特徴とする機器操作権管理システム。

【請求項３０】　請求項２７から２９の何れか１つに記載の機器操作権管理システムにおいて、

前記罰則施行時期を管理する時計は、保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とする機器操作権管理システム。

【請求項３１】　機器操作許可情報を有するＩＣチップであって、

該ＩＣチップには、機器操作許可を有するＩＣカードの所有者のＩＤ番号および操作可能機器情報が記載されていることを特徴とするＩＣチップ。

【請求項３２】　請求項３１に記載のＩＣチップにおいて、

前記ＩＣチップには、機器操作許可を有するＩＣカードの所有者の指紋や網膜・虹彩等の生体認証情報が記載されていることを特徴とするＩＣチップ。

【請求項３３】　請求項３１に記載のＩＣチップにおいて、

前記ＩＣチップには、電子マネー機能も併せて含むことを特徴とするＩＣチップ。

【請求項３４】　請求項３１に記載のＩＣチップにおいて、

前記ＩＣチップには、機器が搭乗および移動可能な機器である場合に、機器の移動に伴う位置や、該位置に到達した時刻等の情報が記録されることを特徴とするＩＣチップ。

【請求項３５】　請求項３１に記載のＩＣチップにおいて、

前記ＩＣチップには、機器の使用におけるルール違反等に対する罰則として、機器操作の一定期間の禁止を含み、時間軸に沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能な情報を含むことを特徴とするＩＣチップ。

【請求項３６】　請求項３１に記載のＩＣチップにおいて、

ＩＣチップには、機器の使用におけるルール違反等に対する罰則として、機能の制限を含み、時間軸に沿って機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能な情報を含むことを特徴とするＩＣチップ。

【請求項３７】　請求項３１から３６の何れか１つに記載のＩＣチップにおいて、

前記ＩＣチップは、ＩＣカード内のＩＣチップであることを特徴とするＩＣチップ。
【請求項３８】　請求項３１から３６の何れか１つに記載のＩＣチップにおいて、
前記ＩＣチップは、機器を始動する鍵に内蔵されることを特徴とするＩＣチップ。
【請求項３９】　請求項３１から３６の何れか１つに記載のＩＣチップにおいて、
前記ＩＣチップには、前記罰則施行時期を管理する時計を内蔵し、この時計は保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とするＩＣチップ。
【請求項４０】　請求項３９に記載のＩＣチップにおいて、
前記時計を駆動する電池の寿命は、機器操作許可の期限と略等しい寿命であることを特徴とするＩＣチップ。
【請求項４１】　機器を取り扱う権利を表示する許可表示手段に記載した情報を読み取る読み取り手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理端末において、
機器の操作許可を得ている者に発行した前記許可表示手段に記載されているＩＤ番号を少なくとも１つ以上記憶する記憶装置を有することを特徴とする機器操作権管理端末。
【請求項４２】　請求項４１に記載の機器操作権管理端末において、
前記機器操作権管理端末内の前記記憶装置に記憶されているＩＤ番号と一致したＩＤ番号の前記許可表示手段を有する者に、前記記憶装置に新たなＩＤ番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理端末。
【請求項４３】　半導体メモリもしくはＣＰＵで構成されたＩＣチップを内蔵したＩＣチップケースであって、
ＩＣカード内の前記ＩＣチップは電気的な接点部分を除いて絶縁体にて封印されており、前記ＩＣチップの電気的な接点の露出部のみを除くように、前記絶縁体の外面全体を導電体で覆った形状で構成されることを特徴とするＩＣチップケース。
【請求項４４】　請求項４３記載のＩＣチップケースにおいて、
前記ＩＣチップの電気的な接点の露出部と、前記導電体を結ぶ直線の間には、前記絶縁体が必ず存在することを特徴とするＩＣチップケース。
【請求項４５】　半導体メモリもしくはＣＰＵで構成されたＩＣチップを内蔵する、機器を取り扱う権利を表示する許可表示手段と、該表示許可手段と接続可能なインタフェースを有する、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
前記ＩＣチップは、情報の暗号化・復号化を行う機能を有し、前記インタフェースには、前記ＩＣチップと同等の機能を有するＩＣチップもしくはアプリケーションソフトウェアを搭載し、前記許可表示手段に内蔵したＩＣチップと、前記インタフェースとの間の通信を、暗号化された信号により行うことを特徴とする機器操作権管理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、機器の操作の可否を管理・制御する機器操作権管理システムにかかわる技術に関し、特に、自動車の免許証等に代表されるライセンスカード形態の機器操作権を表記する機能を有するデバイスと、同デバイスと連携して機器操作者本人であることを生体認証情報を用いて照合する機能などを有する、機器操作権管理システムにかかわる技術に関するものである。
【０００２】
【従来の技術】機器を操作する権利を有することを証明する証明書を発行し、その証明書を保有する者のみが、当該機器の操作を可能とするような、機器操作権管理方法は、各所で利用されている。例えば運転免許証の場合、免許証を持つ者のみが自動車を運転する権利を有し、警察官による運転免許証の提示指示が出たときは、速やかにこれに従い、従えない場合は罰則を科すシステムとして実運用されている。
【０００３】しかし、自動車の運転免許証は、警察官の提示指示があるとき以外は、その効力を発揮することはなく、免許証を持っていなくても、実際には自動車の運転は可能であり、機器操作権を確実に管理するには至っていない。
【０００４】この問題を解決するために、特開平６－８７２８５号公報に開示された技術では、運転免許証としてＩＣカードを用い、このＩＣカードには、ドライバーのＩＤ等の免許証に記載されている事項を電子情報として記入し、自動車にはこの情報を読み取る端末を設け、有効な免許証でない限り、この自動車の運転が出来ないようにし、且つ、ＩＣカード内に運行記録を記入して、後に各ドライバーの稼動状況を集計する方式が記載されている。
【０００５】
【発明が解決しようとする課題】上記した先願公報に開示された技術においては、警察官に提示するとき以外に効力を持たなかった免許証を、自動車が常に判別することで、自動車を運転する権利を示す免許証としての確実な運用が可能になり、併せてＩＣカードのメモリ機能の特徴を生かして、運行状況のログを取り、最適な運行計画に反映させることも可能になる。
【０００６】しかし、前記先願公報に開示された技術では、下記に示すような問題があり、これらの点への配慮がなされていない。
【０００７】①まず、前記先願公報では、自動車にＩＣ

カード免許証を挿入した者が、本当に免許証の所有者かどうかを確認することに関しては、何らの配慮も払われていない。したがって、免許証の交付を受けた者と運転者とが同一人でない場合でも、すなわち、実際には免許が与えられていない者でも、免許証を所持さえしていれば、運転が可能になる。

【０００８】②また、前記先願公報では、交通違反等により免許証を失効したときの対応については、交通事故や交通違反時に、データ管理装置を用いて、免許証内に事故や違反データを書き込みすることや、出頭命令書や反則金納付書を発行することや、あるいは、免許停止・失効中には、免許証を自動車の端末に差し込んでもエンジンがかからないようにすることに関する記述はあるものの、これらは現行の免許証運用方法にのっとったものであって、ＩＣカードを利用することにより初めて得られるメリットを、罰則に適用した検討についてはなされていない。

【０００９】③また、前記先願公報では、自動車のＩＣカード端末に、この自動車を運転することが出来る運転手のＩＤリストを有し、このＩＤと一致する運転手のみが運転できる旨は記載されてはいるものの、免許証の種類と運転可能な自動車の種類及び運転モード種類との連携については、その検討が全くなされていない。

【００１０】④さらに、前記先願公報では、ＩＣカード内容の違法な変更に対して防護を施すことに関しても、何らの配慮も払われていない。

【００１１】本発明は上記の点に鑑みなされたもので、その目的とするところは、機器を操作するライセンスとその所有者が同一であることを、確実に認証可能とすることにある。また、本発明の目的とするところは、操作の違反を行った場合の操作制限について、木目細かく、より実質に沿った処置が可能なようにすることにある。また、本発明の目的とするところは、ライセンスのレベルにより機器操作の制限を細かく設定することを可能とし、以って、確実な機器操作者の管理と、誤操作を防止できるようにすることにある。また、本発明の目的とするところは、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止することにある。

【００１２】

【課題を解決するための手段】上記した目的を達成するために、本発明では、例えば以下のような手段を用いる。

【００１３】（１）自動車にＩＣカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋や虹彩等の生体認証情報を検知する生体認証情報の検出手段を設け、前記ＩＣカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。

【００１４】（２）特に自動車の場合は、通行中に違反を受けて、前記先願公報に記載のような処理を受けると、違反を起こした場所で自動車の運転が不可能になり、車の移動が不可能となってしまう。そこで、ＩＣカード内に、違反時の自動車の運転許可パターンを細かく時間軸に沿って設定することで、例えば、実際の免許停止処分の発行を２日後に設定し、自動車の端末もその指示に沿って動作する。

【００１５】（３）ライセンスのレベルにより、運転する車の動作モードを規定する。例えば、教習所等の専用コースや駐車場において、速度１０ｋｍ／ｈ未満の走行のみが行えるライセンスの設定を行い、自動車の端末もその指示に従って動作する。

【００１６】（４）ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能とする。具体的には、上記（２）、（３）記載の免許停止処分の発行日程やライセンスレベルを、外部に特別な暗号処理チップを用いることなく読み出せ、且つその情報の破壊・改変を防止する。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【００１８】図１は、本発明の第１実施形態に係る機器操作権管理システムの構成を示すブロック図であり、本実施形態は、自動車における機器操作権管理システムへの適用例である。本システムは、機器（ここでは自動車）の動作の可否を制御する機器制御機能をもつ装置と、機器を取り扱う権利（ここでは運転免許であり、例えば、教習所内などの限定されたエリアのみでの運転を許可するものを含むものとする）を示す情報をもつ許可表示手段としてのＩＣカードとを、少なくとも含むものとなっている。

【００１９】自動車にはＩＣカードリーダ10010 があり、ドライバーは自動車を運転する際に、自身のＩＣカードをＩＣカードリーダ10010 に差し込む。生体認証情報リーダ10020 は、運転席に座ったドライバーの指紋もしくは虹彩・網膜などの人間自身のＩＤを示す生体認証情報を読み取る。ライセンス管理装置10040 は、前記ＩＣカードリーダ10010 によってＩＣカードから読取られた、該当免許証の所有者の情報と、同じく前記生体認証情報リーダ10020 によって読み取られた、運転席に座ったドライバーの生体認証情報とを比較し、同一であるかどうかの判断を行う。

【００２０】記憶装置10030 は、例えばこの車両を運転してもよいドライバーを限定するときに、そのドライバーＩＤを記憶する。差し込まれたＩＣカードのドライバーＩＤが、この記憶装置10030 に記憶されたドライバーＩＤと一致しないときは、後述する車両制御装置10060 によりエンジン始動を抑制する。

【００２１】ライセンス管理装置10040 が、差し込まれ

たＩＣカードからの情報と生体認証情報リーダ10020 からの情報とにより、運転席に座ったドライバーが確かにこの自動車を運転する資格を有する本人と判断したとき、ライセンス管理装置10040は、車両制御装置10060 に動作許可を示すメッセージを送る。

【００２２】車両制御装置10060 は、この許可メッセージに従って、エンジン始動の可否を含めてエンジンの制御を行うエンジン制御装置10070 や、自動車の走行速度のリミッターを制御するスピード制御装置10080 や、ＡＢＳ（Antilock Brake System ）の動作、レベルを設定するブレーキ制御装置10090に、それぞれ動作許可指示を送る。これによりエンジンの始動が可能になり、またドライバーの資格レベルに従った最高速度の設定、さらに、現行の免許証制度では存在しないがドライバーの技量に見合った形でＡＢＳのＯＮ／ＯＦＦ制御を行う。

【００２３】図２は、本実施形態の機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の１例を示した説明図である。

【００２４】20000 はコックピットである。運転席右にＩＣカード挿入口20020 があり、この自動車を運転するドライバーは、自身の免許証であるＩＣカードをこの挿入口20020 に挿入する。次に、指紋読み取り部兼エンジン始動ボタン20030 を押すことで、ドライバーの指紋を読み取り、先のＩＣカードに記載したドライバーの生体認証情報との認証を行う。そして、紋読み取り部兼エンジン始動ボタン20030を押した人が、確かにＩＣカードの示す本人であることを認識して、初めてエンジンの始動が行える。

【００２５】このとき、記憶装置20050 に、この自動車を操縦してもよいドライバーのＩＤリストを持つことにより、挿入したＩＣカードのＩＤとの照合を行い、図１の説明と同様に、操縦許可のないドライバーでは、自動車のエンジン始動を含む操作が出来ないようにして、盗難防止等のセキュリティを確保することが出来る。

【００２６】生体認証情報の確認手法としては、スピードメーター位置に網膜・虹彩センサ20010 を設ける方法もある。この場合、ドライバーが運転席に座らない限りは、このセンサを用いて検出することが出来ないので、例えば先の指紋読み取り部兼エンジン始動ボタン20030 を、ＩＣカード（免許証）を交付された本人が助手席から押して、免許証がない人が運転席に座って運転するようなことが、不可能になる。ここで、スピードメーターはドライバーの視線が必ず行くところであり、且つドライバーシートは頭の位置がほぼ固定されるので、網膜・虹彩センサ20010 を設置するのに適している。

【００２７】また、ここで免許証として利用するデバイスは、ＩＣカードであり、電子マネー等で使用するマルチアプリケーション対応のＩＣカードである。これにより、同じＩＣカード内に、電子マネーや電子クレジット等のアプリケーションを同居させることが出来、自動車から料金自動支払いシステム20040 へのアクセスによって、高速道路の自動料金支払いや、ドライブスルーやガソリンスタンド等の必ず自動車に乗車している条件下で買物を行うシステムへの対応を行うことも出来る。

【００２８】さらに、ここで使用する免許証がＩＣカードを用いずに、従来の印刷物による免許証を利用しても、カード挿入口に免許証を挿入して、ＩＤ番号等をイメージスキャナで読み取ることで、この自動車の操縦許可を得ているドライバーの免許証かどうかの判断を行うことが出来る。さらに記憶装置10030 に、ドライバーの生体認証情報を記録しておくことで、ＩＣカードを用いなくても、従来の免許証システムで、免許証と生体認証情報によるドライバー本人との照合を行うことも可能であり、ＩＣカードではなく従来の免許証システムをそのまま用いても、本発明の機能を実現することが出来る。

【００２９】図３は、本実施形態の機器操作権管理システムにおいて用いるＩＣカードの内部構成（ＩＣカードに搭載したＩＣチップの内部構成）の１例を示す説明図である。

【００３０】ＩＣカード30000 に搭載したＩＣチップ30005 は、ＭＦ30010 （Master File）をルートとして、その下位に複数のＤＦ（Dedicated File）を有し、ＤＦ１(30020)は免許証、ＤＦ２(30060)は例えば電子マネーに用いられている。ＤＦ１(30020)の下には複数のＥＦ（Elementary File ）があり、電子免許証に関連する情報が記載されている。ＥＦ１(30030)には、免許証ＩＤ番号と、生体認証情報を示す指紋情報や虹彩情報などがある。この場合、生体認証情報は複数種類あってもよく、自動車の端末に装着された生体認証情報リーダ10020 が、例えば指紋スキャナであった場合は、指紋情報を用い、虹彩センサであるならば、虹彩情報を用いればよい。ＥＦ２(30040)には、この免許証のライセンス種類やレベルが、そしてＥＦ３(30050)には、違反履歴が記載される。ＣＰＵカードは、ＤＦやＥＦがプログラムになっており、外部から特定のコマンドを入力するときのみ、生体認証情報を読み出したり、違反履歴を書き換えたりすることが出来る。この特定のコマンドは、専用のソフトや後述する専用のチップのみが行い、これによりカードの内部情報の機密を保ち、改変を防止することが出来る。

【００３１】また、ここでカード内に時計30070 を設け、前記生体認証情報や違反履歴と同様に、専用のソフトやチップを介さない限り、この時計の日付・時刻を改変出来ない仕掛けとすることで、図４にて後述する、違反時の罰則発行を日付に従って施行する際に、故意に時計を狂わせて罰則発行を免れるような行為を完全に防止することが出来る。カード上で単体で動作する時計のため、当然狂いが生じるが、これはカードを車載の端末に挿入したときに、専用のソフトもしくはチップがＧＰＳ等の確実に信頼できる時計により確認した正しい時刻を

用いて、カード内の時計の狂いを修正する。この時刻の修正は、自動車に搭載した端末に限らず、図２に示した料金自動支払い時の通信において行ってもよく、また自動車に関係なく、電子マネー端末と連携して、電子マネーや電子クレジットによる買物を行った際に、端末から時計の修正を随時行ってもよい。また、ＩＣカード内に設置された時計は、ＩＣカードの駆動電源を外部から与えられなくても動作する必要があり、薄型電池をＩＣカード内に内蔵する。この電池の寿命は、基本的に免許の許可期限以上の寿命とするが、場合によっては、免許の許可期限と略同程度の寿命を持つようにしてもよい。時計の駆動以外ではこの電池は一切使用しないので、使用条件により寿命が短くなるという現象は起きず、正確に寿命の設定をすることが可能である。

【００３２】図４は、本実施形態における、違反時の罰則処理パターンの１例を示す表図である。

【００３３】罰則処理のパターンとして、本実施形態では、自動車を運転する際の動作モードを、（１）エンジン始動のみ、（２）１０ｋｍ／ｈ未満の走行、（３）通常走行可能の３つに分類した。例えば無違反の場合は、当然ながらこの３つの動作モードをすべて使うことが可能である。

【００３４】まず、従来の免許停止に相当するスピード違反について示す。従来の免許証では、スピード違反による罰則すなわち免許停止は即時発行するが、例えば旅行途中でスピード違反をした場合には、そのまま乗って帰ることになり、さらに警察に見つからなければ、そのまま乗り続けることも現実には可能となってしまう。そこで、例えばＩＣカード等による電子情報として違反情報を記載し、自動車にこれに対応する端末を設け、免許停止を即時発行した場合は、その場で例えば半年間のあいだ、自動車を動かすことが出来なくなり、道の真ん中で車を置き去りにするという現象が発生する。本実施形態では、スピード違反をした後、その罰則の発行を違反時から例えば２日後からと設定し、その間に自動車を自宅に持ち帰ったり、貸出し元に返却したりする。その上で実際の罰則が発行されて、この免許証では運転が出来ないような処理をすることが出来る。

【００３５】また、即時免許停止が必要なほど異常なスピード違反を行った場合、少なくとも高速道路のサービスエリア上の道端から、駐車エリアまでは車の移動が出来るように、１０ｋｍ／ｈ以下の走行のみを例えば２日間の一定期間だけ可能とし、一般道路の通常走行の禁止は即時発行する。

【００３６】また、酒気帯び運転による免許停止発行の場合は、少なくとも摘発時点では車の走行は即時やめさせる必要があるので、１０ｋｍ／ｈ以下の走行は勿論、自動車のエンジン始動も不可能とする。これは摘発されたドライバーが酔いから醒めるまでの期間として、例えば６時間だけ完全な運転禁止とし、その後、前記したスピード違反と同様に２日間だけ通常走行を可能として、自宅に車を持ち帰った後、免許停止が初めて発行される。この期間はドライバーの自宅までの距離や情状酌量に応じて、摘発した担当者が決定することが出来る。

【００３７】なお、ＩＣカードに書き込む罰則による制限事項は、時間軸に沿って、使用許可、使用禁止、使用機能制限などを複数回にわたって設定可能となっている。

【００３８】本実施形態における罰則発行の時期・時刻は、ある基準となる時計に従って施行されるが、例えば通常の自動車に搭載された時計を用いた場合、ドライバーが勝手にその時計を変更し、例えば時計を半年進めてしまえば、すでに処分期間は過ぎているので、勝手に運転をすることが可能となってしまう。これを防ぐために、図３に示したように、外部から勝手に時刻の変更を行えないような時計をＩＣカード内に持ったり、同様な機能、すなわちＧＰＳ等の確実に信頼できる時計により時刻の修正を行う以外は、任意の時刻設定がまったく出来ないような時計を、車載の端末に持たせてもよい。

【００３９】図５は、本発明の第２実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の１例を記述した表図である。本実施形態はヘリコプターの操縦を想定した例であり、正規ライセンスのパイロット、訓練生、そしてメカニックそれぞれのライセンスと、それぞれに対する動作モードを示している。

【００４０】正規ライセンスのパイロットは、当然ながらエンジン始動、ホバリング、低速飛行、高速飛行のすべてを行うことが出来る。訓練生の場合は、エンジン始動から低速飛行までが行え、高速飛行への制限がある。具体的には、例えばメインローター回転面の角度を、パイロットの意志では一定以上傾けることが出来ないような制御を入れる。勿論ジャイロ等による自動姿勢制御はこの制限を受けずに、角度一杯まで倒すことが可能である。また、簡単な浮上試験が出来る資格を持つメカニック１級はエンジン始動及びホバリングまで可能とする。具体的には、極低速の前後左右移動までが可能な程度に、例えばメインローター回転面の角度の変更操作が不可能となるような制御を行う。整備資格のみを持つメカニック２級の場合はエンジン始動のみである。

【００４１】このような制御の具体的な制限手法は、操縦する機器により異なるが、ＩＣカード免許にライセンスのレベルを記載し、実際に操作する機器側で、そのライセンスでどこまで操作出来るかを設定することで、例えば自動車を運転する際、同じ仮免許証でも、一般道路と専用コース内で動作モードを変えるような制御が可能である。

【００４２】図６は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第１例である。

【００４３】まず、操作する機器にＩＤカードを挿入し（ステップ60010 ）、次に指紋の入力を行う（ステップ60020 ）。次に、ステップ60030 にて、挿入したＩＤカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＤカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＤカードのEject を行う（ステップ60040 ）。照合結果が○であれば、エンジンスタートを行い（ステップ60050 ）、操縦する機器が自動車であれば、走行を行う（ステップ60060 ）。

【００４４】ここで、例えばＩＤカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号等をイメージスキャナで読み取り、図１、図２で示した機器に搭載されている記憶装置から、該当免許証番号に対応した指紋情報を読み出して、操縦者が入力した指紋との一致判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【００４５】図７は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第２例と第３例である。

【００４６】図７の（ａ）は、ＩＤカードと操縦する機器の種類の照合を行う場合のフローチャートである。まず、操縦者は機器にＩＤカードを挿入し（ステップ70010 ）、操縦する機器は挿入されたＩＤカードからライセンスＩＤを読取る。そして、該当ライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70020 ）、操縦が出来ない場合は運転不可表示を行い、且つＩＤカードのEject を行う（ステップ70030 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70040 ）、操縦する機器が自動車であれば、走行を行う（ステップ70050 ）。

【００４７】ここで、例えばＩＤカードは前記した如く、メモリを持つＩＣチップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号及び記載されている操縦可能機器の種類をイメージスキャナで読み取り、本機器を操縦できるライセンスかどうかの判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【００４８】図７の（ｂ）は、図６と図７の（ａ）の両方の機能を実現した例を示すフローチャートである。すなわち、操縦者は機器にＩＤカードを挿入し（ステップ70010 ）、次に指紋の入力を行う（ステップ70060 ）。次に、ステップ70070 にて、挿入したＩＤカードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者がＩＤカードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、ＩＤカードのEject を行う（ステップ70031 ）。照合結果が○であれば、挿入されたＩＤカードから読み取ったライセンスＩＤが、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70021）、操縦が出来ない場合は運転不可表示を行い、且つＩＤカードのEject を行う（ステップ70032 ）。照合結果が○であれば、エンジンスタートを行い（ステップ70041 ）、操縦する機器が自動車であれば、走行を行う（ステップ70051 ）。

【００４９】ここで、指紋照合とライセンスＩＤの照合順序は、どちらでも構わないが、例えば自動車において、指名手配者等のライセンスＩＤをネットワーク等で自動車が常に受信している場合、この照合時点にて自動車は搭乗しているドライバーが犯罪者等であることを認識し、運転不可表示を行うと同時に、図示しない通信手段を用いて、犯罪者の存在を警察等に知らせるという仕掛けを実現することも出来る。この手順を一番最初に行うことで、確実な犯罪者の検知を行うことが可能となる。

【００５０】なおまた、指紋照合などの生体認証情報の認証（照合）は、自動車等の乗り物の所定の扉の取っ手に指紋読み取りセンサを設けることなどにより、乗り物に搭乗する際の、扉の開閉操作と同時に行うようにしてもよい。

【００５１】さらにまた、指紋や虹彩などの生体認証情報の認証（照合）は、自動車などの機器の起動前毎に行うだけでなく、機器の起動開始許可後に、一定時間毎に行うようにしたり、あるいは、機器の動作終了時毎に行うようにしてもよい。このようにすることで、機器の動作を立ち上げた後に、最初に認証した人物と異なる者が、途中で機器の運転や操縦などを交代したかどうかを監視することができる。そして、途中で運転や操縦などを交代した場合には、自動車等の機器がこの旨を警告したり、時と場合によるが警告後に機器の動作を徐々に停止させたり、あるいは、ＩＣカードや機器の記憶装置に、不正交代したことの情報と交代後の人物の生体認証情報とを併せて記録したり、または、不正交代したことの情報と交代後の人物の生体認証情報とを外部に自動報知したりするような、仕組みとすることもできる。したがって、タクシーなどにおいて、悪意の乗客が車を乗っ取って運転した時などにおいて、大いにその効力を発揮する。

【００５２】図８は、本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードリーダおよび生体認証情報リーダを装着してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【００５３】図８の（ａ）に示したリモコンは、リモコンにＩＣカードリーダと生体認証情報リーダとしての指紋スキャナとを具備させることにより、前記した第１実施形態における機器制御機能をもつ車載の装置（端末装置）と同等の機能を持たせたものである。

【００５４】リモコン本体には、指紋スキャナ兼スターターボタン80020 があり、利用者がＩＣカード80030 を

差し込んで、ボタン80020 に指を乗せることで指紋のスキャンを行い、ＩＣカード80030 内に記載した指紋情報とスキャンした利用者の指紋情報との照合を行って、照合が成立したときに初めて、赤外線／電波発射口80010 より、自動車のエンジンスタートやドアロック解除等の信号を、赤外線もしくは電波によって発射する。

【００５５】図８の（ｂ）は、ＩＣカードの機能をリモコンの内部に内蔵した例である。この例の場合、汎用の自動車の免許証とは異なる使用形態になるが、ある機器を動かそうとしたときに、その機器を動かす資格のある者の指紋情報を記憶しているので、他の者が機器を動かそうとしてもスタート出来ない。また、ＩＣカードの差し込みがないのでカードの携帯による紛失を回避することも出来る。

【００５６】図９は、本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。具体的な例として、ある自動車のオーナーが、その自動車を運転する権利を他の人に与えるための操作フローを、操作画面を元に説明する。

【００５７】まず、図９の（ａ）の操作画面で示すように、自動車は他人への運転許可を与える人が、確かにその車のオーナーかどうかの判定をするために、オーナーにＩＤカードの挿入を促す。ここで、図示しない指紋等の生体認証情報の照合により、オーナー本人であることを確認する。

【００５８】次に、図９の（ｂ）に示す操作画面で、他人に与える運転許可モードを選択する。すなわち、

「１」を選択することで当日のみ、「２」を選択することで指定日付を指定する。そして、「３」を選択することで、例えば家族などの永久ライセンスを与える。この選択の後、図９の（ａ）と同様な操作画面にて、運転許可を与えるドライバーのＩＤカードの挿入を促し、運転許可の登録を行う。

【００５９】図９の（ｃ）の画面は、現在この車に既に登録されている運転可能ドライバーの一覧を表示したものを示す。ここで番号により選択を行うことで、図９の（ｄ）の操作画面に示すように、運転許可モードの変更を行うことが出来る。

【００６０】図１０は、本発明による機器操作権管理システムにおいて、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。生体認証情報の認証（照合）は、例えば指紋照合の方式では、現状、代表的なものとして次の３方式がある。

①．指紋の稜線の分岐点、端点の位置と方向を照合するマニーシャア方式。

②．①に加え、相対的な位置関係を用いるマニーシャアリレーション方式。データ量と処理負荷が大きいが、警察庁が犯人を割り出すのに使用している。

③．特徴点を含む画像片（チップ）を用いて照合する画像チップ方式。

【００６１】方式としての認証精度は、②→③→①の順となっている。また、その各々に対して、どれだけサンプリングするかで照合精度が変化し、サンプリング数を上げると処理時間がかかる。照合精度の取り方としては、例えば、特徴点を１５箇所くらい選んで、これを順次照合し、７箇所連続して一致すれば照合作業完とする。このように特徴点の数と、照合をどこまでで止めるかで照合精度が決まり、例えば全部照合すると時間もかかり、逆に本人照合率が低下することもある。

【００６２】基本的に、ライセンスの種類により操縦できる機器が確実に限定されるのが、目標であり理想であるが、上記の問題により認証精度を上げると、処理時間がかかったり、逆に本人でも認証してくれないという現象が発生する。操縦する機器の種類によっては、本人認証のレベルを下げてもよいものがあり、処理速度の向上やコストの削減に対応することが可能になる。

【００６３】図１０の表は、操縦する車種とその重要度とライセンスの資格レベルを示す。重要度はＣがもっとも低く、Ａがもっとも重要度が高い。また、資格レベルはＥがもっとも低く、Ａがもっとも高くて、高いレベルのライセンスを持つ者は低いレベルのライセンスの運転資格も同時に有する。例えば普通免許証をＤとし、原動機付自転車の免許証をＥとすると、Ｄの免許証を持つ者は原動機付自転車の運転も可能である。

【００６４】図１０の表において、重要度がＣの原動機付自転車は、その操縦資格レベルも最低のＥであるので、免許証を持っている者ならほとんどの者が操縦可能な機器である。そこで生体認証情報の認証も精密にやる必要がなく、生体認証レベルを最低のレベル「１」としてある。

【００６５】普通自動車やタクシー、大型車は、車両のコストも高価で盗難による影響も大きいので、重要度をＢとする。その中で普通車は一般個人車両であるので、その資格レベルはＤ、タクシーは業務車両であるので、その資格レベルをＣとする。この２つは、車両の大きさおよび操縦の難易度は同じであるため、生体認証レベルは同じとして、原動機付自転車よりも高いレベル「２」に設定する。

【００６６】大型車は、前記２つの車両に比べて大きく、運転も難易度が高いため、より確実な資格が必要（資格レベルＢ）になるということで、生体認証レベルをさらに高いレベル「３」に設定する。

【００６７】そして最後に、緊急自動車は、重要度がＡともっとも高く、特定の資格者のみが操縦するということで、資格レベルも最高のＡとする。そして盗難が発生したときの影響がもっとも大きいので、より確実なドライバーの確認を行うために、生体認証レベルを最高の「４」とする。この場合、緊急車両は緊急出動が必要と

なるため、確実な認証と同時に、有資格者を間違えずに短時間で確実に認証する必要がある。このため、生体認証のアルゴリズムもそれに適したものを利用することになる。

【００６８】図１１は、本発明による機器操作権管理システムにおいて、ＩＣカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。すなわち、図１に示した前記第１実施形態の機器操作管理システムを用いて自動車を運転する者が、その走行経路を自身の記録として、ＩＣカードに保存する方法を示した説明図である。

【００６９】図１１の（ａ）は、ドライバーがたどる経路を示している。出発点11040 から、道路11030 を通過して交差点11020 を左折した後、Ｙ字分岐11010 を左折して、目的地11000 に到着する。この通行経路は、あらかじめカーナビゲーションシステムにより設定しておくが、通行時に、交差点11020 の様子を電子カメラで撮影する（11060 は、この撮影画像を示している）。画像上に重ねた矢印11070 は、実際に自動車が曲がった方向である。

【００７０】図１１の（ｂ）は、ドライバーの通行経路をドライバーのＩＣカードに記録するフォーマットの例である。通行路を、交差点を主に、いくつかのチェックポイント別に分離し、始点座標と終点座標を緯度・経度で表記し、始点を通過した日付・時刻と、このルートを通行するのに要した時間とを記載する。さらに、交差点のマークとなるように、図１１の（ａ）で撮影した画像のファイル名を添付する。この記録は、走行中に一旦車載の記憶装置に記録して、最後にＩＣカードにダウンロードするようにしてもよい。

【００７１】このような記録を行うことにより、ＩＣカード（特にＣＰＵカード）の守秘性により、改変しない正確な走行記録を、走行した個人の管理下に置くことが可能となり、個人的な管理および、例えば同一の車種および外観の自動車が犯罪を起こしたときに、この記録により自身が犯罪とは関係ないことを証明することも可能となる。

【００７２】図１２は、本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。

【００７３】図１２の（ａ）は、鍵120010にＩＣチップ120020を内蔵させ、インタフェース端子120030によって、この鍵120010と鍵を挿入する自動車の端末とを接続するように構成した例である。この場合、免許証とは形態は異なるが、鍵自身に前述した如くドライバーのＩＤ番号や生体認証情報を入れておくことで、現状と同様の鍵の使用のみで、ＩＣカードの利用と同様な効果をもたせることができる。

【００７４】図１２の（ｂ）は、鍵120011に、図１２の（ａ）の鍵120010の機能に加えて、さらに指紋センサ120040を内蔵させた例である。なお、図１２の（ｂ）において、120021はＩＣチップ、120031はインタフェース端子である。

【００７５】この図１２の（ｂ）の例の場合には、鍵120011を自動車の鍵穴に挿入し、ひねってエンジンをかけるという現在の操作とまったく同じ操作で、前記した実施形態と同様の効果を得ることができる。ここで、指紋センサ120040に代替する生体認証情報センサとして、個人によって微妙に異なる指の荷重分布を情報として検出するセンサを用いてもよい。また、荷重分布も面方向だけではなく、鍵をひねる際の時間軸による荷重変化を生体認証情報として用いてもよい。鍵を持つ・ひねるという操作を利用することで、指紋センサという高度なセンサを用いなくても、生体認証情報の認証を行うことが可能である。

【００７６】図１３は、本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。図１３の表のフォーマットは、図４、図５と同様のためここでの説明は省略する。

【００７７】免許証の種類は練習生、仮免許、本免許、そしてＡＴ（オートマチック車）限定を示す。例えば、教習所内でのみの運転を行う練習生は、エンジン始動も含めてすべて△とする。これは、操作は可能であるが、助手席に本免許証を有するものが搭乗している条件で運転が可能ということを示す。助手席に本免許証を有するものがいることの証明は、教習専用の車で、運転席と同様のＩＣカードリーダーを助手席に設置する方法と、図９で示した運転許可を与えるのと同様に、事前に本免許証を運転席の端末に差し込んで、認証を行った上で、練習生に運転許可を与える方法がある。仮免許による運転許可も同様である。

【００７８】本免許は当然すべての自動車の操縦ができるが、ここでＡＴ限定免許の者は、そのライセンスの種類により、ＡＴ車の走行は可能であるが、ＭＴ車の走行は不可能となる。具体的には、ギアを入れるとスロットルが開かないように、もしくはエンジンストールをするような仕掛けとする。ただし、緊急脱出用にスターターモーターによる走行を可能としたり、５分以内の速度１０ｋｍ／ｈ未満の走行のみを可能とするような制御を行ってもよい。

【００７９】図１４は、本発明による機器操作権管理システムにおいて適用可能な、端末装置へのＩＣカード挿入時におけるＩＣチップの静電破壊を防止するための、ＩＣカードの実施形態の例を示した説明図である。

【００８０】140060は端末（端末装置）側のＩＣカード挿入口であり、挿入時にコネクタ140061にて、ＩＣカード側の電極と接続する。ＩＣカード140000は、その芯が絶縁体で構成され、ＩＣチップ140010が封入されて電極部のみが表面に露出されている。そして、ＩＣカード14

0000はその周囲を導電体140030が覆っており、導電体とＩＣチップの間にはスパーク等が生じないように一定の間隔があくように、且つ、導電体とＩＣチップとの間にスパークが飛ぶような空間が存在せず、必ず絶縁体がさえぎる形で入るように絶縁体140020の形状が設定されている。

【００８１】ＩＣカード140000を利用者が持つと、導電体140030は人体を通じてアースされる（140040）。ＩＣカードを端末に挿入するときに、特に自動車等の場合は、アースに相当する路面との間がゴムタイヤで絶縁されているため、帯電した自動車と挿入したＩＣカードとの間（140070）にスパークが生じる。このスパークがＩＣチップ140010に流れ込まないように、導電体140030を通して人体経由でアースさせることで、端末とＩＣカードの電位を等しくする。また、端末内のＩＣカードスロットには導電ブラシ140050を設け、特にＩＣカードの端子表面の除電や埃の清掃等を行う。これにより、特に自動車特有の高電圧静電気によるＩＣカード（ＩＣチップ）の破損を防止することができる。

【００８２】図１５は、本発明による機器操作権管理システムにおいて適用可能な、端末（端末装置）とＩＣカード間の情報の守秘を行う実施形態の例を示した説明図である。

【００８３】端末150000（端末装置）とＩＣカード150100の間の情報は、例えば図１４に示した接点をモニターすることで、傍受が可能である。さらに傍受した信号を解析することで、この接点から擬似的な信号を入力して、ＩＣカード記載事項の改変を行うこともできる。

【００８４】そこで、図１５に示した本例では、ＩＣカード150100のＩＣチップに、ＣＰＵ内蔵チップを用い、端末150000との間の信号の授受を暗号化した信号で行う。端末150000側には、ＩＣカードに内蔵したチップと同等の機能を持つＣＰＵ内蔵チップ150010、もしくは、専用アプリケーション150020があり、ＩＣカードとの通信をこれらのチップもしくはアプリケーション経由にて行う。ＩＣカード150100に内蔵のＩＣチップと、端末150000側のＩＣチップもしくはアプリケーションは同じ方式による暗号化・復号化機能を有し、ＩＣカード150100の情報の読み出し、書き換え等のコマンドおよび情報の傍受、並びにこれらに基づく改変や偽造を、確実に防止する。免許証番号や氏名等、通常の免許証の記載事項と同等で、秘密にする必要のない情報は、スルー経路150030を通して読み出すことができる。この場合は、例えば電子マネーの残高表示機と同様に、ごく簡単な構造の端末で情報の表示を行うことができる。また、暗号処理を行わなくても、ＣＰＵチップの使用により、ＩＣカードへの書き込みアクセスに特定のコマンドを使用することが可能となり、簡便に誤操作や破壊を防止することが可能となる。

【００８５】以上、本発明を主として図示した実施形態によって説明したが、当業者には本発明の精神を逸脱しない範囲で種々の変形が可能であることは言うまでもなく、例えば、ＩＣカードとして接触式で情報を授受するもの以外にも、ＩＣカードに至近距離間での無線送受信が可能な機能を具備させて、非接触で情報を授受するタイプのものを用いることも可能である。この場合、本発明のＩＣチップの機能を、携帯電話や腕時計などの携帯機器に内蔵させることも可能である。

【００８６】

【発明の効果】以上のように本発明によれば、機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うことが出来る。また、操作の違反を行った場合の操作制限も、時間軸に沿った木目細かい処理を行うことが出来、より実質に沿った処置をすることが出来る。また、ライセンスのレベルにより、機器操作の制限を細かく設定することが出来、確実な機器操作者の管理と誤操作を防止することが可能となる。さらに、ＣＰＵカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能となる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る機器操作権管理システムの構成例を示すブロック図である。

【図２】本発明の第１実施形態に係る機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の１例を示す説明図である。

【図３】本発明の第１実施形態に係る機器操作権管理システムにおいて用いる、ＩＣカードの内部構成の１例を示す説明図である。

【図４】本発明の第１実施形態に係る機器操作権管理システムにおける、違反時の罰則処理パターンの１例を表で示す説明図である。

【図５】本発明の第２実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の１例を表で示した説明図である。

【図６】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第１例を示すフローチャート図である。

【図７】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第２例および第３例を示すフローチャート図である。

【図８】本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードリーダおよび生体認証情報リーダを具備してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【図９】本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。

【図１０】本発明による機器操作権管理システムにおい

て、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。

【図１１】本発明による機器操作権管理システムにおいて、ＩＣカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。

【図１２】本発明による機器操作権管理システムにおいて適用可能な、ＩＣカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。

【図１３】本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。

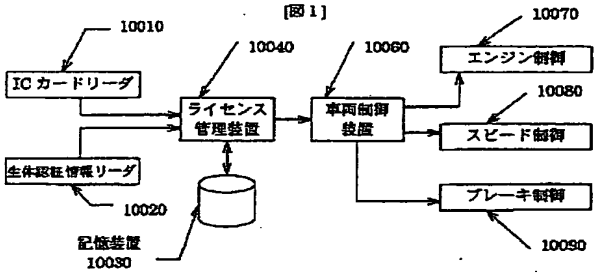
【図１４】本発明による機器操作権管理システムにおいて適用可能な、端末装置へのＩＣカード挿入時におけるＩＣチップの静電破壊を防止するための、ＩＣカードの実施形態の例を示した説明図である。

【図１５】本発明による機器操作権管理システムにおいて適用可能な、端末（端末装置）とＩＣカード間の情報の守秘を行う実施形態の例を示した説明図である。

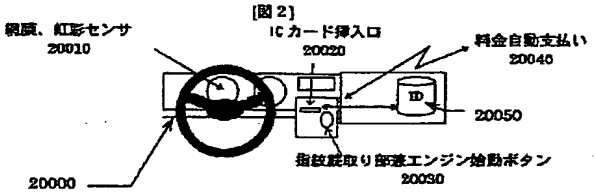
【符号の説明】

10010　ＩＣカードリーダ
10020　生体認証情報リーダ
10030　記憶装置
10040　ライセンス管理装置
10060　車両制御装置
10070　エンジン制御装置
10080　スピード制御装置
10090　ブレーキ制御装置
20000　コックピット
20010　網膜・虹彩センサ
20020　ＩＣカード挿入口
20030　指紋読み取り部兼エンジン始動ボタン
20040　料金自動支払いシステム
20050　記憶装置
30000　ＩＣカード
30005　ＩＣチップ

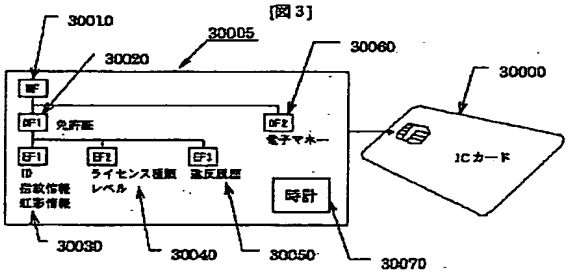
【図１】



【図２】



【図３】



【図４】

[図4]

#	事項	動作モード		
		エンジン始動	10km/h 未満	通常走行
1	無違反	○	○	○
2	スピード違反	○	○	○(但２日間)
3	重大スピード違反	○	○(但２日間)	×
4	酒気帯び運転	×(但６時間)	×(但６時間)	○ (但６時間以降２日間)

【図５】

[図5]

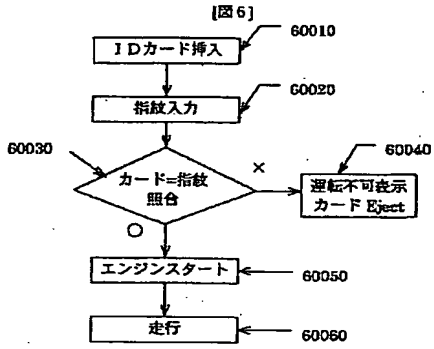
#	事項	動作モード			
		エンジン始動	ホバリング	低速飛行	高速飛行
1	パイロット	○	○	○	○
2	武装ヘリ	○	○	○	×
3	メカニック１級	○	○	×	×
4	メカニック２級	○	×	×	×

【図１０】

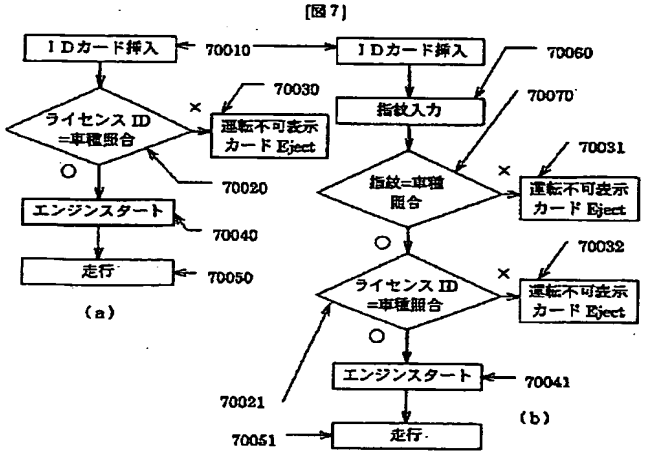
[図10]

#	車種	ライセンス管理レベル		
		重要度	資格レベル	生体認証レベル
1	原動機付自転車	C	E	1
2	普通車	B	D	2
3	タクシー等	B	C	2
4	大型車	B	B	3
5	緊急自動車	A	A	4

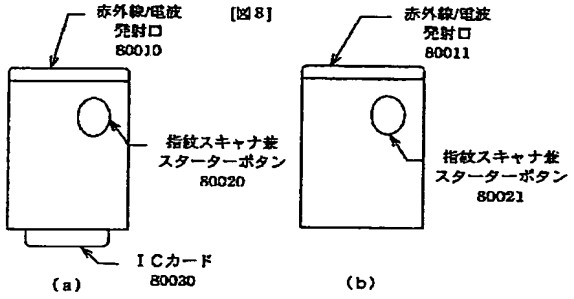
【図６】



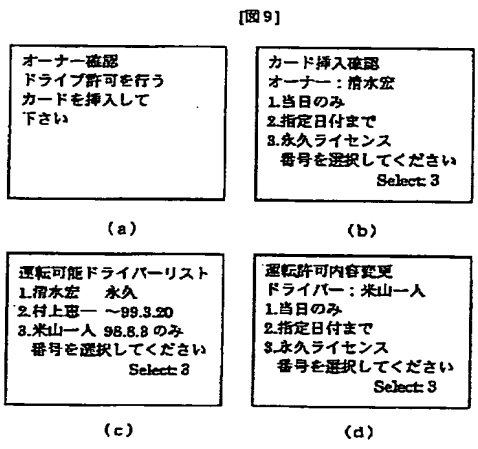
【図７】



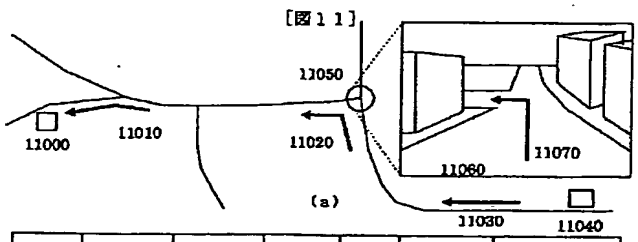
【図８】



【図９】



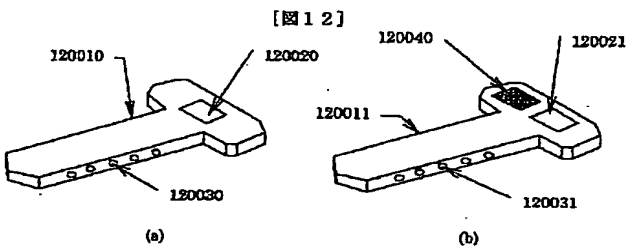
【図１１】



ルート#	終点座標	始点座標	日付	時刻	所要時間	画像ファイル名
1	110.25-540.12	111.32-538.00	H10.7.30	14:00	8分	W0001.GIF
2	111.32-538.00	112.21-535.86	H10.7.30	14:08	7分	W0002.GIF
.....						
8	120.00-532.65	122.37-533.77	H10.8.2	07:59	１２分	W0008.GIF
.....						
22	131.88-525.07	130.02-522.98	H10.8.6	16:45	１５分	W0022.GIF
23	130.02-522.98	129.25-521.45	H10.8.6	17:00	１６分	W0023.GIF

(b)

【図１２】



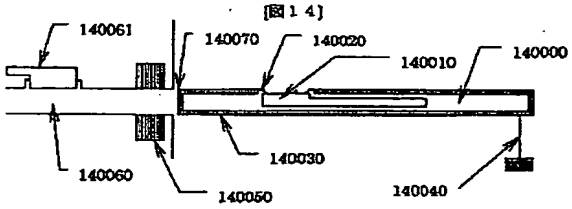
【図１３】

[図１３]

#	事項	動作モード		
		エンジン始動	ＭＴ	ＡＴ
1	練習生	△	△	△
2	仮免許	○	△	△
3	本免許	○	○	○
4	ＡＴ限定	○	×	○

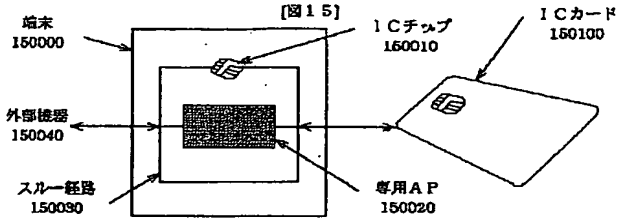
【図１４】

[図１４]



【図１５】

[図１５]



フロントページの続き

(51) Int. Cl. 7　　識別記号　　Ｆ Ｉ　　ﾃｰﾏｺｰﾄﾞ (参考)
Ｇ０７Ｆ　7/08　　Ｇ０７Ｆ　7/08　　Ａ

(72)発明者　松本　健司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考)　2C005 MA25 MB01 MB03 MB08 QA01 SA02 SA05 SA15
3E044 AA20 BA04 CA06 CA10 DA05
5B035 AA14 BB09 BC03 CA11
5B043 AA04 AA09 BA02 FA04 GA01
5B058 KA38 YA13

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.